# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 54, Task ID: 207

Task ID: 207 Risk Level: 5

Date Processed: 2016-04-22 06:01:56 (UTC)

Processing Time: 61.16 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\1af5338669efabe0a9841478396871b1.exe"

Sample ID: 54
Type: basic
Owner: admin

Label: 1af5338669efabe0a9841478396871b1

 Date Added:
 2016-04-22 06:01:55 (UTC)

 File Type:
 PE32:win32:gui

File Size: PE32:win32:gui

MD5: 1af5338669efabe0a9841478396871b1

SHA256: 98511820966946e5c2c543c720816047a808816f674bc8525016f362785c8b3e

Description: None

# Pattern Matching Results

2 ECMA Script

- 3 Connects to local host
- 5 JavaScript: Writes a string of text to a document stream
- 3 HTTP connection response code 200 (success)
- 3 Long sleep detected
- 4 Checks whether debugger is present
- 4 JavaScript: Eval method
- 2 HTML file
- 1 YARA score 1

#### Static Events

YARA rule hit: Nonexecutable

#### Process/Thread Events

Creates process: C:\windows\temp\1af5338669efabe0a9841478396871b1.exe

["C:\windows\temp\1af5338669efabe0a9841478396871b1.exe"]

Calls function: jscript.dll:eval
Calls function: mshtml.dll:document.write

# Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

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

Creates mutex: \Sessions\1\BaseNamedObjects\!IETld!Mutex
Creates mutex: \Sessions\1\BaseNamedObjects\ZonesCounterMutex

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

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

Creates mutex: \Sessions\I\BaseNamedObjects\\_!MSFIHISTORY!

Creates mutex:

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

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

Creates mutey

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

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

Creates mutex: \Sessions\1\BaseNamedObjects\RasPbFile

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

Creates mutex: \Sessions\1\BaseNamedObjects\\_DDrawExclMode\_\_
Creates mutex: \Sessions\1\BaseNamedObjects\\_DDrawCheckExclMode\_\_
Creates mutex: \Sessions\1\BaseNamedObjects\DDrawWindowListMutex
Creates mutex: \Sessions\1\BaseNamedObjects\DDrawDriverObjectListMutex

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

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!mshist012016042220160423!

Creates event: \KernelObjects\MaximumCommitCondition

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

Creates event: \Security\LSA\_AUTHENTICATION\_INITIALIZED
Creates event: \BaseNamedObjects\SvcctrlStartEvent\_A3752DX

Creates event: \BaseNamedObjects\BFE\_Notify\_Event\_{4bbd9a10-487f-433d-8006-

86ec7fc0b76c}

### File System Events

```
C:\Users\Admin
 Creates
 Creates:
                        C:\Users\Admin\AppData\Local
 Creates:
                        {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet\ Files}
 Creates:
                        C:\Users\Admin\AppData\Roaming
                        Creates:
 Creates:
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\History
 Creates:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\TZILKL9J\index[1].php
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\266VNL5S\bd_logo1[1].png
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\nuomi_510f7472[1].png
                        \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet| \\
 Creates:
Files\Content.IE5\TZILKL9J\icons_0e814c16[1].png
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\266VNL5S\all_async_search_641293e1[1].js
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\WM60WM90\zbios_62c636fe[1].png
 Creates:
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\VB8EH8F1\baidu_jgylogo3[1].gif
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches
 Creates:
 Creates
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423
 Creates:
C:\Users\Admin\Favorites
                        C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Creates:
Files\Content.IE5\TZILKL9J\favicon[1].ico
                        C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
                        C:\Windows\Prefetch\1AF5338669EFABE0A984147839687-7F9632B6.pf
 Opens:
                        C:\Windows
 Opens:
 Opens:
                        C:\Windows\System32\wow64.dll
                        C:\Windows\System32\wow64win.dll
 Opens:
 Opens:
                        C:\Windows\System32\wow64cpu.dll
                        C:\Windows\system32\wow64log.dll
 Opens:
 Opens:
                        C:\Windows\SysWOW64
 Opens:
                        C:\Windows\SysWOW64\sechost.dll
 Opens:
                        C:\windows\temp\1af5338669efabe0a9841478396871b1.exe.Local\
                        C:\Windows\winsxs\x86 microsoft.windows.common-
 Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
 Opens:
                        C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
 Opens:
                        C:\windows\temp\MSIMG32.dll
 Opens:
                        C:\Windows\SysWOW64\msimg32.dll
                        C:\windows\temp\VERSION.dll
 Opens:
 Opens:
                        C:\Windows\SysWOW64\version.dll
 Opens:
                        C:\Windows\SysWOW64\imm32.dll
 Opens:
                        C:\Windows\WindowsShell.Manifest
 Opens:
                        C:\windows\temp\msdialg100_D.dll
 Opens:
                        C:\Windows\SysWOW64\msdialg100_D.dll
                        C: \verb|\windows\system\msdialg100_D.dl1| \\
 Opens:
 Opens:
                        C:\Windows\msdialg100_D.dll
 Opens:
                        C:\Windows\SysWOW64\Wbem\msdialg100_D.dll
 Opens:
                        C:\Windows\SysWOW64\WindowsPowerShell\v1.0\msdialg100_D.dll
 Opens:
                        C:\windows\temp\MFC90ENut.dll
 Opens:
                        C:\Windows\SysWOW64\MFC90ENut.dll
 Opens:
                        C:\Windows\system\MFC90ENut.dll
 Opens:
                        C:\Windows\MFC90ENut.dll
 Opens:
                        C:\Windows\SysWOW64\Wbem\MFC90ENut.dll
 Opens:
                        C:\Windows\SysWOW64\WindowsPowerShell\v1.0\MFC90ENut.dll
 Opens:
                        C:\windows\temp\Afx100net.dll
 Opens:
                        C:\Windows\SysWOW64\Afx100net.dll
 Opens:
                        C:\Windows\system\Afx100net.dll
 Opens:
                        C:\Windows\Afx100net.dll
 Opens:
                        C:\Windows\SysWOW64\Wbem\Afx100net.dll
                        C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Afx100net.dll
 Opens:
 Opens:
                        C:\program files\fve31bb\zxz63d\Log.dat
 Opens:
                        C:\Program Files\FVe31bb\ZXz63d\BLr11610Ho64.dll
                        C:\Windows\SysWOW64\rpcss.dll
 Opens:
 Opens:
                        C:\Windows\SysWOW64\uxtheme.dll
 Opens:
                        C:\Users\Admin\AppData\Local\Temp\restart.dat
 Opens:
                        C:\windows\temp\dwmapi.dll
 Opens:
                        C:\Windows\SysWOW64\dwmapi.dll
 Opens:
                        C:\Windows\Fonts\StaticCache.dat
                        C:\Windows\Fonts\tahoma.ttf
 Opens:
 Opens:
                        C:\Windows\Fonts\meiryo.ttc
 Opens:
                        C:\Windows\Fonts\msgothic.ttc
```

```
Opens:
                          C:\Windows\Fonts\msjh.ttf
 Opens:
                          C:\Windows\Fonts\msvh.ttf
 Opens:
                          C:\Windows\Fonts\malgun.ttf
 Opens:
                          C:\Windows\Fonts\mingliu.ttc
 Opens:
                          C:\Windows\Fonts\simsun.ttc
 Opens:
                          C:\Windows\Fonts\gulim.ttc
                          C:\Windows\SysWOW64\en-US\user32.dll.mui
 Opens:
 Opens:
                          C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens:
                          C:\Windows\SysWOW64\uxtheme.dll.Config
 Opens:
                          C:\program files\fve31bb\zxz63d\log.dat
 Opens:
                          C:\Windows\SysWOW64\ieframe.dll
 Opens:
                          C:\Windows\SysWOW64\oleacc.dll
 Opens:
                          C:\windows\temp\OLEACCRC.DLL
                          C:\Windows\SysWOW64\oleaccrc.dll
 Opens:
 Opens:
                          C:\Windows\Temp\1af5338669efabe0a9841478396871b1.exe
 Opens:
                          C:\Windows\SysWOW64\ole32.dll
 Opens:
                          C:\windows\temp\ntmarta.dll
 Opens:
                          C:\Windows\SysWOW64\ntmarta.dll
 Opens:
                          C:\Windows\SysWOW64\en-US\urlmon.dll.mui
                          C:\Windows\SysWOW64\shell32.dll
 Opens:
 Opens:
                          C:\windows\temp\apphelp.dll
 Opens:
                          C:\Windows\SysWOW64\apphelp.dll
 Opens:
                          C:\Windows\SysWOW64\en-US\ieframe.dll.mui
 Opens:
                          C:\WINDOWS\Temp\MJPGC.TMP
 Opens:
                          C:\Windows\SysWOW64\wininet.dll
 Opens:
                          C:\windows\temp\profapi.dll
 Opens:
                          C:\Windows\SysWOW64\profapi.dll
 Opens:
                          C:\Users\Admin
 Opens:
                          C:\Users\Admin\AppData\Local
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
                          {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
 Opens:
Files\Content.IE5
                          {\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}
 Opens:
Files\Content.IE5\desktop.ini
                          C:\Users\Admin\AppData\Roaming
 Opens:
                          C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Opens:
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\History
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
 Opens:
                          C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\History\History.IE5| \\
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
 Opens:
                          C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
 Opens:
                          C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
 Opens:
\label{lem:c:start} C: \label{lem:c:start} Admin\ App Data \ Local\ Microsoft\ Windows\ History\ . IE5\ index.\ dat
                          C:\windows\temp\dnsapi.DLL
 Opens:
                          C:\Windows\SysWOW64\dnsapi.dll
 Opens:
 Opens:
                          C:\windows\temp\iphlpapi.DLL
 Opens:
                          C:\Windows\SysWOW64\IPHLPAPI.DLL
 Opens:
                          C:\windows\temp\WINNSI.DLL
 Opens:
                          C:\Windows\SysWOW64\winnsi.dll
 Opens:
                          C:\windows\temp\RASAPI32.dll
                          C:\Windows\SysWOW64\rasapi32.dll
 Opens:
 Opens:
                          C:\windows\temp\rasman.dll
 Opens:
                          C:\Windows\SysWOW64\rasman.dll
 Opens:
                          C:\windows\temp\rtutils.dll
 Opens:
                          C:\Windows\SysWOW64\rtutils.dll
 Opens:
                          C:\ProgramData\Microsoft\Network\Connections\Pbk\
 Opens:
                          C:\Windows\SysWOW64\ras
 Opens:
                          C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
 Opens:
                          C:\windows\temp\sensapi.dll
                          C:\Windows\SysWOW64\SensApi.dll
 Opens:
 Opens:
                          C:\Windows\SysWOW64\nlaapi.dll
 Opens:
                          C:\windows\temp\rasadhlp.dll
                          C:\Windows\SysWOW64\rasadhlp.dll
 Opens:
 Opens:
                          C:\Windows\SysWOW64\mswsock.dll
                          C:\Windows\SysWOW64\WSHTCPIP.DLL
 Opens:
 Opens:
                          C:\windows\temp\MLANG.dll
 Opens:
                          C:\Windows\SysWOW64\mlang.dll
                          C:\Program Files (x86)\Common Files\microsoft shared\ink\tiptsf.dll
 Opens:
 Opens:
                          C:\Windows\SysWOW64\wship6.dll
 Opens:
                          C:\windows\temp\dhcpcsvc6.DLL
                          C:\Windows\SysWOW64\dhcpcsvc6.dll
 Opens:
 Opens:
                          C:\windows\temp\dhcpcsvc.DLL
 Opens:
                          C:\Windows\SysWOW64\dhcpcsvc.dll
 Opens:
                          C:\Windows\System32\drivers\etc\hosts
 Opens:
                          C:\Windows\SysWOW64\FWPUCLNT.DLL
```

 $\label{linear_lambda} $$C:\Users\Lambda \end{subarray} Admin\end{subarray} Admin\end{subarray} at $$Cookies\Lambda \end{subarray} at $$Cookies$ 

```
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
                         C:\Windows\System32\C 20127.NLS
 Opens:
 Opens:
                         C:\Windows\SysWOW64\mshtml.dll
                         C:\Windows\SysWOW64\msls31.dll
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\index[1].php
                         C:\Windows\SysWOW64\msimtf.dll
 Opens:
                         C:\Windows\SysWOW64\jscript.dll
 Opens:
 Opens:
                         C:\windows\temp\CRYPTSP.dll
                         C:\Windows\SysWOW64\cryptsp.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\rsaenh.dll
 Opens:
                         C:\windows\temp\RpcRtRemote.dll
 Opens:
                         C:\Windows\SysWOW64\RpcRtRemote.dll
                         C:\Windows\SysWOW64\iepeers.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\winspool.drv
 Opens:
                         C:\Windows\SysWOW64\dxtrans.dll
 Opens:
                         C:\Windows\SysWOW64\atl.dll
 Opens:
                         C:\Windows\SysWOW64\ddrawex.dll
 Opens:
                         C:\Windows\SysWOW64\ddraw.dll
                         C:\Windows\SysWOW64\dciman32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\en-US\setupapi.dll.mui
 Opens:
                         C:\Windows\win.ini
                         C:\Windows\SysWOW64\en-US\ddraw.dll.mui
 Opens:
 Opens:
                         C:\Windows\SysWOW64\dxtmsft.dll
 Opens:
                         C:\windows\temp\SXS.DLL
                         C:\Windows\SysWOW64\sxs.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\kernel32.dll
 Opens:
                         C:\Windows\Fonts\arial.ttf
 Opens:
                         C:\Windows\SysWOW64\en-US\mlang.dll.mui
 Opens:
                         C:\Windows\System32\C_1250.NLS
 Opens:
                         C:\Windows\System32\C_1251.NLS
                         C:\Windows\System32\C_1253.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_1254.NLS
                         C:\Windows\System32\C_1255.NLS
C:\Windows\System32\C_1256.NLS
 Opens:
 Opens:
 Opens:
                         C:\Windows\System32\C_1257.NLS
 Opens:
                         C:\Windows\System32\C_1258.NLS
                         C:\Windows\System32\C_874.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_932.NLS
 Opens:
                         C:\Windows\System32\C_936.NLS
                         C:\Windows\System32\C_949.NLS
 Opens:
 Opens:
                         C:\Windows\System32\C_950.NLS
 Opens:
                         C:\Windows\System32\C_1361.NLS
 Opens:
                         C:\Windows\Fonts\arialbd.ttf
 Opens:
                         C:\Windows\Fonts\ariali.ttf
 Opens:
                         C:\Windows\SysWOW64\en-US\mshtml.dll.mui
 Opens:
                         C:\windows\temp\ImgUtil.dll
 Opens:
                         C:\Windows\SysWOW64\imgutil.dll
                         C:\Windows\SysWOW64\pngfilt.dll
 Opens:
 Opens:
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
 Opens:
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
                         C:\windows\temp\D3DIM700.DLL
 Opens:
 Opens:
                         C:\Windows\SysWOW64\d3dim700.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\jscript.dll.mui
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\266VNL5S\all_async_search_641293e1[1].js
                         C:\Windows\SysWOW64\tzres.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\en-US\tzres.dll.mui
 Opens:
                         C:\Windows\SysWOW64\urlmon.dll
 Opens:
                         C:\
 Opens:
                         C:\Windows\SysWOW64\propsys.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001.db
 Opens:
                         C:\Users\desktop.ini
 Opens:
                         C:\Users
 Opens:
                         C:\Users\Admin\AppData
                         C:\Users\Admin\AppData\Local\Microsoft
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History.IE5\MSHist012016042220160423\
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042220160423\index.dat
                         C:\Windows\SysWOW64\en-US\shell32.dll.mui
 Opens:
 Opens:
                         C:\Users\Admin\Favorites
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\TZILKL9J\favicon[1].ico
 Writes to:
```

```
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt
 Writes to:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Writes to:
Files\Content.IE5\TZILKL9J\index[1].php
```

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

Files\Content.IE5\266VNL5S\bd\_logo1[1].png

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

Files\Content.IE5\VB8EH8F1\nuomi\_510f7472[1].png

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

Files\Content.IE5\TZILKL9J\icons\_0e814c16[1].png

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

Files\Content.IE5\266VNL5S\all\_async\_search\_641293e1[1].js

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

Files\Content.IE5\WM60WM90\zbios\_62c636fe[1].png

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

Files\Content.IE5\VB8EH8F1\baidu\_jgylogo3[1].gif

Writes to:

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

Files\Content.IE5\TZILKL9J\favicon[1].ico

Writes to: C:\Users\Admin\AppData\Local\Temp\httpwww.baidu.comfavicon.ico

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

Reads from: C:\Windows\Temp\1af5338669efabe0a9841478396871b1.exe

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

Reads from: C:\Windows\win.ini

Reads from: C:\Windows\SysWOW64\dxtmsft.dll Reads from: C:\Windows\SysWOW64\dxtrans.dll

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

Files\Content.IE5\266VNL5S\all\_async\_search\_641293e1[1].js

Reads from: C:\Users\desktop.ini

Reads from: C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini Reads from:  ${\tt C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary\ Internet}$ 

Files\Content.IE5\TZILKL9J\favicon[1].ico

Deletes:

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[1].txt

Deletes:

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\admin@baidu[2].txt

#### Network Events

DNS query: www.baidu.com DNS query: s1.bdstatic.com www.a.shifen.com ⇒ 103.235.46.39 DNS response: wwwstatic1.gshifen.com ⇒ 103.235.44.90 DNS response: Connects to: 8.8.8.8:53 Connects to: 103.235.46.39:80 Connects to: 127.0.0.1:65465 Connects to: 103.235.44.90:80 Sends data to: 8.8.8.8:53 Sends data to: 127.0.0.1:65465 Sends data to: www.a.shifen.com:80 (103.235.46.39) Sends data to: wwwstatic1.gshifen.com:80 (103.235.44.90) Receives data from: 8.8.8.8:53 Receives data from: 127.0.0.1:65465 Receives data from: www.a.shifen.com:80 (103.235.46.39) Receives data from: wwwstatic1.gshifen.com:80 (103.235.44.90)

## Windows Registry Events

Creates key: HKCU\software\explore

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

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

Creates key:

HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasapi32

Creates key:

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

settings\connections

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

awareness

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ runmru$ Creates key:

Creates key: HKCU\software\microsoft\internet explorer\typedurls

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\typedpaths

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

settings\p3p\history

Creates key: HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication

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

Creates key:  $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| direct 3d\\| most recent application$ 

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

settings\5.0\cache\extensible cache\mshist012016042220160423

HKCU\software\microsoft\internet explorer\main\windowssearch Creates key:

Creates kev: HKLM\software\wow6432node\microsoft\downloadmanager Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings\zonemap[proxybypass]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

Deletes value: 

settings\zonemap[intranetname]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options

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

Opens key: HKLM\software\microsoft\wow64

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

execution options

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

Opens kev:

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

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

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

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

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

Opens key: HKCU\

 $\label{thm:local_machine} \begin{tabular}{ll} HKCU \control panel \desktop \muicached \machine \label{thm:local_machine} anguage configuration \end{tabular}$ Opens key: Opens key:  $HKLM \verb|\system| current controlset| control \verb|\mui| settings \verb|\language| configuration$ 

Opens key: HKCU\software\policies\microsoft\control panel\desktop  ${\it HKCU} \ control\ panel\ desktop\ language configuration$ Opens key:

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

Opens key:

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

 $\label{lem:hklm} \verb+Kklm \+ system \+ control \+ ls \+ sorting \+ versions$ Opens key:

Opens key: HKLM\

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

nt\currentversion\diagnostics

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

nt\currentversion\gre\_initialize

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

nt\currentversion\compatibility32

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

compatibility

Opens key:

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

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

Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\wow6432node\microsoft\oleaut HKLM\system\currentcontrolset\services\crypt32 Opens key:

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

settings Opens key:

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

settings

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

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

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

Opens key: HKLM\system\currentcontrolset\control\nls\locale

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

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

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore\_v1.0

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui

HKLM\system\currentcontrolset\control\cmf\config Opens kev: Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\fontsubstitutes

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

```
HKLM\software\microsoft\windows
    Opens kev:
nt\currentversion\languagepack\surrogatefallback\ms shell dlg
                                                                           HKCU\software\explore
     Opens key:
     Opens key:
                                                                           HKCU\software\classes\
     Opens key:
                                                                           HKLM\software\microsoft\com3
                                                                           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}
     Opens key:
                                                                           HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
                                                                           HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-
     Opens key:
00c04fd705a2}\treatas
     Opens key:
                                                                           HKCR \setminus wow 6432 node \\ clsid \\ \{8856f961-340a-11d0-a96b-00c04fd705a2\} \\ \\ \\ treatas
     Opens key:
                                                                           HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{8856f961-340a-11d0-a96b-12d1\} \\ \cap (3856f961-340a-11d0-a96b-12d1) 
00c04fd705a2}\progid
     Opens key:
                                                                           HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid
                                                                           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\software\wow6432node\microsoft\rpc
     Opens key:
                                                                           HKLM\system\currentcontrolset\control\computername\activecomputername
     Opens key:
                                                                           HKLM\system\setup
     Opens key:
                                                                           HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
                                                                           HKLM\software\policies\microsoft\windows nt\rpc
     Opens key:
     Opens key:
                                                                           HKLM\software\policies\microsoft\sqmclient\windows
     Opens key:
                                                                           HKLM\software\microsoft\sqmclient\windows
                                                                           HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{889d2 \\ feb-5411-4565-8998-1000 \\ node 
     Opens key:
 1dd2c5261283}
     Opens key:
                                                                           HKCR\wow6432node\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
                                                                           HKCU\software\classes\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
     Opens key:
     Opens key:
                                                                           HKCR\clsid\{889d2feb-5411-4565-8998-1dd2c5261283}
     Opens key:
                                                                           HKCU\software\policies\microsoft\windows\app management
     Opens key:
                                                                           \label{lem:hklm} \begin{tabular}{ll} HKLM \end{tabular} wow 6432 node \end{tabular} policies \end{tabular} microsoft \end{tabular} wow 6432 node \end{tabular} policies \end{tabular} wow 6432 node 
     Opens key:
                                                                           HKLM\software\policies\microsoft\windows\app management
     Opens key:
                                                                           HKCU\software\classes\wow6432node\clsid\{004b0726-a010-4abf-8556-
 fcdb7f1fca1e}
     Opens key:
                                                                           HKCR\wow6432node\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
     Opens key:
                                                                           HKCU\software\classes\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e}
                                                                           HKCR\clsid\{004b0726-a010-4abf-8556-fcdb7f1fca1e\}
     Opens key:
     Opens key:
                                                                           Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                                                          Opens key:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                                                           HKLM\software\wow6432node\microsoft\ctf\
     Opens key:
     Opens key:
                                                                           HKLM\software\wow6432node\microsoft\ctf\knownclasses
     Opens key:
                                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings
                                                                           HKCU\software\microsoft\windows\currentversion\internet settings
     Opens key:
                                                                           HKCU\software\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_http_username_password_disable
                                                                          HKLM\software\wow6432node\microsoft\internet
     Opens key:
 explorer\main\featurecontrol\feature_http_username_password_disable
     Opens key:
                                                                          HKLM\software\wow6432node\policies\microsoft\internet
 explorer\main\featurecontrol
     Opens key:
                                                                           \label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ internet explorer \+ main \+ feature control
                                                                           HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
     Opens kev:
     Opens key:
                                                                          HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol
     Opens key:
                                                                          HKCU\software\microsoft\internet explorer\main\featurecontrol
                                                                          HKCU\software\microsoft\internet
     Opens key:
 explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
     Opens key:
                                                                          HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                                                          HKCU\software\microsoft\internet
     Opens kev:
 explorer\main\featurecontrol\feature use ietldlist for domain determination
     Opens key:
                                                                          HKLM\software\wow6432node\microsoft\internet
 explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
     Opens kev:
                                                                          HKLM\svstem\currentcontrolset\control\lsa\accessproviders
     Opens key:
                                                                           HKLM\system\currentcontrolset\services\ldap
     Opens key:
                                                                           HKCU\software\microsoft\internet explorer\ietld
     Opens key:
                                                                           HKLM\software\wow6432node\microsoft\internet explorer\main
     Opens key:
                                                                           HKLM\software\wow6432node\policies\microsoft\internet explorer\main
```

HKLM\software\policies\microsoft\internet explorer\main

HKCU\software\policies\microsoft\internet explorer\main

Opens key:

Opens kev:

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

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

Opens key:

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

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

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

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

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

Opens key:

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

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

08002b30309d}\inprocserver32

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

08002b30309d}\inprocserver32

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: HKCU\software\microsoft\windows\currentversion\shell extensions\cached Opens key: HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}

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

08002b30309d}\treatas

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

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

08002b30309d}\progid

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

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

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

08002b30309d}\progid

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

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

08002b30309d}\inprochandler32

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

08002b30309d}\inprochandler32

 $Opens~key: \\ HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{871c5380-42a0-1069-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-10$ 

08002b30309d}\inprochandler

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

08002b30309d}\inprochandler

Opens key:

42a0-1069-a2ea-08002b30309d}

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

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

explorer\main\featurecontrol\feature\_iedde\_register\_protocol

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

settings\accepted documents

Opens key:

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

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

Opens key: HKCU\software\microsoft\internet

Opens key: HKLM\software\wow6432node\policies

Opens key: HKCU\software\policies
Opens key: HKCU\software

Opens key: HKLM\software\wow6432node

Opens key:

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_ignore\_policies\_zonemap\_if\_esc\_enabled\_kb918915

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

 $explorer \verb|\main| feature control| feature \_ignore \_policies \_zonemap \_if \_esc \_enabled \_kb918915$ 

Opens key:

settings\zonemap\domains\

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

settings\zonemap\domains Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_unc\_savedfilecheck Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_unc\_savedfilecheck Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\ HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_zones\_check\_zonemap\_policy\_kb941001 Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_zones\_check\_zonemap\_policy\_kb941001 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zonemap Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\ranges\  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Opens kev: settings\zonemap\protocoldefaults\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\domains\ Opens key: settings\zonemap\domains\  $HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus internet \ explorer$ Opens key: Opens key: HKLM\software\policies\microsoft\internet explorer 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  $\label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\sl}} \mbox{\tt zones\sl} \mbox{\tt 2}$ Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\ HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones Opens key:  $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\zones\ Opens key:  $HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet \ settings \ vones \ \ 0$ HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zones\0  $\label{lem:hkcu} \verb+KCU\software\policies\microsoft\windows\currentversion\notation{ \columnwidth}{line} \begin{tabular}{ll} \columnwidth \columnwi$ Opens key: settings\zones\0 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1 HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\1 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\1 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zonemap\ Opens kev: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\2  $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\zones\2 Opens kev:  $HKLM \ software \ wow 6432 node \ policies \ microsoft \ windows \ current version \ internet\ settings \ vones \ \ 3$ HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zones\3 HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\3 Opens kev: HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\4

HKCU\software\policies\microsoft\windows\currentversion\internet

settings\zones\4
 Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature\_localmachine\_lockdown

```
Opens key:
                                                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
     Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
    Opens key:
                                                                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones
    Opens key:
                                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\lockdown_zones\
     Opens key:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
     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\0
    Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                                                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
    Opens kev:
 settings\lockdown_zones\0
                                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
    Opens key:
 settings\lockdown_zones\0
                                                                           HKCU\software\microsoft\windows\currentversion\internet
     Opens key:
settings\lockdown_zones\1
    Opens kev:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\lockdown_zones\1
                                                                           HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens key:
 settings\lockdown_zones\1
                                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
    Opens key:
 settings\lockdown_zones\1
                                                                           HKCU\software\microsoft\windows\currentversion\internet
     Opens key:
settings\lockdown_zones\2
    Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus internet \setminus microsoft \setminus windows \setminus current version \setminus microsoft \setminus micr
settings\lockdown_zones\2
                                                                           Opens key:
 settings\lockdown_zones\2
                                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
    Opens kev:
 settings\lockdown_zones\2
                                                                           HKCU\software\microsoft\windows\currentversion\internet
     Opens key:
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 key:
 settings\lockdown_zones\3
    Opens key:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown zones\4
     Opens key:
HKLM \verb|\software\\| wow 6432 node \verb|\policies\\| microsoft\\| windows\\| current version\\| internet | microsoft\\| windows\\| current version\\| current versi
settings\lockdown zones\4
    Opens key:
                                                                           HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\lockdown_zones\4
                                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
    Opens kev:
 settings\lockdown_zones\4
    Opens key:
                                                                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache
    Opens key:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
 settings\5.0\cache\content
                                                                           HKLM\software\wow6432node\microsoft\windows\currentversion\internet
     Opens key:
settings\5.0\cache\content
     Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
    Opens key:
HKLM \label{lem:hklm} White the software \label{lklm} White the 
33be-4251-ba85-6007caedcf9d}
     Opens kev:
33be-4251-ba85-6007caedcf9d}\propertybag
                                                                           HKCU\software\microsoft\windows\currentversion\explorer
     Opens kev:
     Opens key:
                                                                           HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
     Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in follows folders
     Opens key:
                                                                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders
                                                                           HKLM\software\wow6432node\policies\microsoft\windows\explorer
     Opens kev:
     Opens key:
                                                                           HKLM\software\policies\microsoft\windows\explorer
     Opens key:
                                                                           HKCU\software\policies\microsoft\windows\explorer
     Opens kev:
```

 $\label{thm:hcm.software} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(f1b32785-b). The software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(f1b32785-b). The software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(f1b32785-b). The software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescription\explorer\folderdes\explorer\fo$ 

```
6fba-4fcf-9d55-7b8e7f157091}
    Opens kev:
6fba-4fcf-9d55-7b8e7f157091}\propertybag
HKLM \label{lem:hklm} White the latest and the la
0e22-4760-9afe-ea3317b67173}
   Opens key:
0e22-4760-9afe-ea3317b67173}\propertybag
                                                        HKLM\software\wow6432node\microsoft\windows
    Opens kev:
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
   Opens key:
                                                        980053277-1733835069-2361817685-1001
    Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
                                                       HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\5.0\cache\cookies
                                                        HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\cache\cookies
    Opens key:
c0e9-4171-908e-08a611b84ff6}
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-164644, 2b0f765d-16464, 2b0f766d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b0f76d-16464, 2b0
c0e9-4171-908e-08a611b84ff6}\propertybag
65f9-4cf6-a03a-e3ef65729f3d}
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
                                                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
                                                        HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet
    Opens key:
settings\5.0\cache\history
   Opens kev:
b784-432e-a781-5a1130a75963}
    Opens key:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-descriptions\} \ description \ explorer \ folder \ descriptions \ explorer \ folder \ 
b784-432e-a781-5a1130a75963}\propertybag
                                                        HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\5.0\cache\extensible cache
                                                        HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\5.0\cache\extensible cache\domstore
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
                                                       HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\5.0\cache\extensible cache\iecompat
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
    Opens key:
                                                        HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
                                                       HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                                                        HKLM\software\wow6432node\microsoft\internet
    Opens key:
explorer\main\featurecontrol\retry headeronlypost onconnectionreset
    Opens key:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
    Opens key:
                                                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
                                                        HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature skip post retry on internetwritefile kb895954
    Opens key:
                                                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
    Opens key:
                                                        \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache
    Opens key:
                                                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
   Opens key:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
    Opens key:
                                                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
    Opens key:
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
   Opens key:
                                                       HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
    Opens key:
                                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
```

HKLM\software\wow6432node\microsoft\internet

```
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
                               HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:
                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:
                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                               HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:
                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:
                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:
                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:
                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:
                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                              HKLM\software\wow6432node\microsoft\internet
  Opens key:
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
                               HKLM\software\wow6432node\microsoft\internet
  Opens key:
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
  Opens key:
                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
                               HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
  Opens key:
                               HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
                               HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                               HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature security flag ignore revocation kb2275828
  Opens key:
                               HKLM\system\currentcontrolset\services\winsock2\parameters
                               HKLM \ system \ \ current controls et \ \ winsock 2 \ \ parameters \ \ \ appid\_catalog
  Opens kev:
  Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ appid\_catalog \ 0.24bd 1 a 1 \ and \ system \ additional to the system \ and \ a
HKLM\svstem\currentcontrolset\services\winsock2\parameters\protocol catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
  Opens kev:
Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens kev:
```

```
Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004
   Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005
   Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\internet settings\wpad
                                                HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature return failed connect content kb942615
   Opens key:
                                                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
   Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 1af5338669 efabe 0a 9841478396871b1\_rasapi 3241478396871b1\_rasapi 32414787506871b1\_rasapi 32414787506871b1\_rasapi 32414787506871b1\_rasapi 32414787506871b1\_rasapi 32414787506871b1\_rasapi 32414787506871b1\_rasapi 32414787506871b1\_rasapi 32414787506871b1\_rasapi 324147506871b1\_rasapi 32414750671b1\_rasapi 32414750671b1\_rasapi 32414750
   Opens key:
HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1_rasmancs
   Opens key:
                                                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
   Opens key:
                                                HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
   Opens key:
                                                HKLM\software\microsoft\sqmclient\windows\disabledsessions\
   Opens key:
                                                HKLM\system\currentcontrolset\control\sqmservicelist
   Opens kev:
   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:
                                                HKCU\software\microsoft\internet explorer
   Opens key:
                                                HKLM\software\wow6432node\microsoft\internet explorer
   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
   Opens key:
                                                HKCU\software\classes\protocols\name-space handler\
   Opens key:
                                                HKCR\protocols\name-space handler
   Opens key:
                                                HKCU\software\classes\protocols\name-space handler\http\
   Opens key:
                                                HKCR\protocols\name-space handler\http
                                                HKCU\software\classes\protocols\name-space handler\*\
   Opens key:
   Opens key:
                                                HKCR\protocols\name-space handler\*
   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
                                                HKCU\software\microsoft\windows\currentversion\internet settings\user
   Opens key:
agent
   Opens key:
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Opens key:
settings\5.0\user agent
   Opens kev:
                                                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\user agent
   Opens key:
                                                \label{lem:hkcu} \verb+KCU\software\policies\microsoft\windows\currentversion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currentersion\currenters
settings\user agent
   Opens key:
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\user agent\ua tokens
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Opens kev:
settings\user agent\pre platform
   Opens key:
                                                settings\5.0\user agent\pre platform
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Opens kev:
settings\user agent\post platform
   Opens key:
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
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_browser_emulation
                                                HKLM\software\wow6432node\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature browser emulation
   Opens key:
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver
   Opens key:
                                                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver
                                                HKCU\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_maxconnectionsper1_0server
```

explorer\main\featurecontrol\feature\_maxconnectionsper1\_0server
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock

HKLM\software\wow6432node\microsoft\internet

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

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

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

migration\providers\tcpip

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

Opens key: HKCU\software\microsoft\internet

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

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

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

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

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

Opens kev:

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

Opens key:

 $\label{thm:cursoft} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \explorer \autocomplete \end{tabular}$ 

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

Opens key:

 $HKLM \verb|\software\policies\microsoft\windows\currentversion\explorer\autocomplete | leading to the constant of the constant o$ 

Opens key:

HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key:

00c04fd7d062}

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens kev:

00c04fd7d062}\treatas

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\progid

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} Opens key:

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\progid

Opens key: HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\inprocserver32

HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key:

00c04fd7d062}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\inprochandler32

HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-Opens key:

00c04fd7d062}\inprochandler32

Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00bb2765 - 6a77 - 11d0 - a535 - 6a77 - 11d0 - a550 - 6a77$ 

00c04fd7d062}\inprochandler

Opens key: HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-

00c04fd7d062}\inprochandler

Opens key: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}

HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\treatas

 $HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{6935db93-21e8-4ccc-beb9-9fe3c77a297a\} \setminus treatas$ Opens key: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-Opens key:

9fe3c77a297a}\progid

Opens key:  $HKCR\wow6432 node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\ \ progid$ Opens key: HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a} Opens key: HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}

Opens key: HKCU\software\classes\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\progid

HKCR\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}\progid Opens key:

Opens key: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\inprocserver32

HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-Opens key:

9fe3c77a297a}\inprocserver32

HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-Opens kev:

9fe3c77a297a}\inprochandler32

HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-Opens key:

9fe3c77a297a}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-

9fe3c77a297a}\inprochandler

HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-Opens kev:

9fe3c77a297a}\inprochandler

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-

00c04fd7d062}

Opens key: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062} Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00bb2764 - 6a77 - 11d0 - a535 - 6a77 - 6a77$ 

00c04fd7d062}\treatas

Opens key:  $HKCR \setminus wow 6432 node \\ clsid \setminus \{00bb2764 - 6a77 - 11d0 - a535 - 00c04fd7d062\} \\ \setminus treat as \\ \setminus \{00bb2764 - 6a77 - 11d0 - a535 - 00c04fd7d062\} \\ \setminus treat \\ \setminus \{00bb2764 - 6a77 - 11d0 - a535 - 00c04fd7d062\} \\ \setminus treat \\ \setminus \{00bb2764 - 6a77 - 11d0 - a535 - 00c04fd7d062\} \\ \setminus \{00bb2764 - 11d0 - 11d0 - 11d0 - a535 - 00c04fd7d062\} \\ \setminus \{00bb2764 - 11d0 -$ 

Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\progid Opens key:  $HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\progid$ HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062} Opens key: Opens key: HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\progid HKCR\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\progid Opens key: Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00bb2764 - 6a77 - 11d0 - a535 - 12d0 - 12d0 + 12d0 - 12d0$ 00c04fd7d062}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{00bb2764-6a77-11d0-a535-Opens kev: 00c04fd7d062}\inprochandler HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-Opens key: 00c04fd7d062}\inprochandler Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid  $HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{00bb2763 - 6a77 - 11d0 - a535 - 00c04fd7d062\} \setminus progid$ Opens key: Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32 HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-Opens kev: 00c04fd7d062}\inprocserver32  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00bb2763 - 6a77 - 11d0 - a535 - 6a77 - 11d0 - a550 - 6a77$ Opens key: 00c04fd7d062}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{00bb2763-6a77-11d0-a535-Opens kev: 00c04fd7d062}\inprochandler HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-Opens kev: 00c04fd7d062}\inprochandler Opens key: HKCU\software\classes\wow6432node\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32 HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-Opens kev: 00aa005b4383}\inprocserver32 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client\ Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997} HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997} Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\treatas Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\progid Opens key:  $HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997\}\progid$ Opens key: HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\inprocserv er32 HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens kev: b61bb7cdd997}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens kev: b61bb7cdd997}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920b61bb7cdd997}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens kev b61bb7cdd997}\inprochandler HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-Opens kev: b61bb7cdd997}\inprochandler Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions Opens key: HKLM\software\microsoft\rpc\extensions Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip6 Opens key:  $HKLM \verb|\software\\| wow 6432 node \verb|\policies\\| microsoft\\| system\\| dnsclient$ Opens key: HKLM\software\policies\microsoft\system\dnsclient

Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-

 $\label{lem:hklm} \verb+Kklm \system \current control set \services \label{lem:hklm} \verb+ dn s cache \services \services$ 

```
e1e01c1f69b5}
                         HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens kev:
 Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
 Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-
127795cce47a}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-
65fee5hae0h1}
 Opens key:
                         HKLM\system\currentcontrolset\services\tcpip\linkage
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history\baidu.com
 Opens key:
                         HKCU\software\classes\mime\database\content type\text/html; charset=utf-
 Opens key:
                         HKCR\mime\database\content type\text/html; charset=utf-8
 Opens key:
                         HKCU\software\classes\mime\database\content type\text/html
 Opens key:
                         HKCR\mime\database\content type\text/html
                         HKCU\software\classes\protocols\filter\text/html; charset=utf-8
 Opens key:
 Opens key:
                         HKCR\protocols\filter\text/html; charset=utf-8
 Opens key:
                         HKCU\software\classes\protocols\filter\text/html
                         HKCR\protocols\filter\text/html
 Opens kev:
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_mime_sniffing
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_feeds
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_safe_bindtoobject
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}
                         HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
 Opens key:
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\treatas
                         HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
 Opens key:
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\progid
                         HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
 Opens key:
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32
                         HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
 Opens key:
00aa00686f13}\inprocserver32
 Opens kev:
                         HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler32
                         HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
 Opens key:
00aa00686f13}\inprochandler32
                         HKCU\software\classes\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
 Opens key:
00aa00686f13}\inprochandler
 Opens key:
                         HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
 Opens key:
                         HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_aria_support
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKCU\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_css_show_hide_events
                                    HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_css_show_hide_events
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_display_node_advise_kb833311
  Opens key:
                                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
                                    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
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:
                                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                                    HKLM\software\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
  Opens key:
                                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:
                                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:
                                    HKCU\software\microsoft\internet
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 key:
explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
  Opens key:
                                    HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_crash_recovery_save_kb978454
                                    HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:
                                    HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_cleanup_at_fls
                                    HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
  Opens key:
explorer\main\featurecontrol\feature_cleanup_at_fls
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\app
  Opens kev:
paths\outlook.exe
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
                                     \label{local-objection} \mbox{HKLM\software\wow6432} node\mbox{\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\sware\
  Opens key:
compatibility
  Opens key:
                                     HKLM\software\wow6432node\policies\microsoft\internet
explorer\domstorage
                                     HKLM\software\policies\microsoft\internet explorer\domstorage
  Opens key:
  Opens key:
                                     HKCU\software\policies\microsoft\internet explorer\domstorage
  Opens key:
                                     HKCU\software\microsoft\internet explorer\domstorage
                                     HKLM\software\wow6432node\microsoft\internet explorer\domstorage
  Opens key:
  Opens key:
                                     HKLM\software\wow6432node\policies\microsoft\internet
explorer\safety\privacie
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
                                     HKCU\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
                                     HKCU\software\microsoft\internet explorer\safety\privacie
                                     \label{thm:local_ham} \begin{tabular}{ll} HKLM \software \wow 6432 node \microsoft \internet explorer \safety \privacie \end{tabular}
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\internet
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\main\featurecontrol\feature_restrict_filedownload
                                    HKLM\software\wow6432node\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature restrict filedownload
                                    HKLM\software\wow6432node\microsoft\internet explorer\security\floppy
  Opens key:
access
  Opens key:
                                     HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
detection
                                     HKLM\software\wow6432node\microsoft\internet explorer\security\adv
  Opens kev:
addrbar spoof detection
                                     HKCU\software\classes\protocols\name-space handler\about\
  Opens key:
  Opens key:
                                     HKCR\protocols\name-space handler\about
                                     . \\ \textbf{HKCU} . \\ \textbf{software} \\ \textbf{classes} \\ \textbf{protocols} \\ \textbf{handler} \\ \textbf{about}
  Opens kev:
```

HKCR\protocols\handler\about

HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-Opens key: 00aa00bdce0b} HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\treatas Opens key:  $HKCR\wow6432 node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treat as$ HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\progid  $HKCR\wow6432 node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\ \ progid$ Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens key: Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\progid Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32 HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-Opens kev:

00aa00bdce0b}\inprocserver32

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

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

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

00aa00bdce0b}\inprochandler

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_document\_compatible\_mode HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_document\_compatible\_mode Opens key: HKCU\software\microsoft\internet

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

explorer\main\featurecontrol\feature\_protocol\_lockdown explorer\main\featurecontrol\feature\_protocol\_lockdown

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

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: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature\_weboc\_document\_zoom

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

settings\url history

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

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\microsoft\internet

explorer\main\featurecontrol\feature\_ipersistmoniker\_load\_redirected\_url\_kb976425

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

explorer\main\featurecontrol\feature\_ipersistmoniker\_load\_redirected\_url\_kb976425 Opens key: HKCU\software\policies\microsoft\internet explorer

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

 $\label{thm:hkcu} \begin{tabular}{ll} HKCU \software \begin{tabular}{ll} \dot{m} & cripts \\ \end{tabular}$ Opens key:

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

explorer\international\scripts

Opens key: HKLM\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

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

Opens key: HKCU\software\microsoft\windows\currentversion\policies Opens key: HKCU\software\microsoft\internet explorer\pagesetup Opens key:  $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\mbox{\sc menuext}} \\$ Opens key: HKCU\software\microsoft\internet explorer\menuext\%s Opens key: HKLM\system\currentcontrolset\control\nls\codepage

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_zone\_elevation

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

explorer\main\featurecontrol\feature\_zone\_elevation 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\windows\currentversion\internet settings\zones

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

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

settings\zones\0

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\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\3

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

settings\zones\4

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_mshtml\_autoload\_ieframe

Opens key:  $\label{lower} \mbox{HKLM\software\wow6432node\microsoft\internet}$ 

explorer\main\featurecontrol\feature\_mshtml\_autoload\_ieframe

Opens key: HKLM\software\www6432node\policies\microsoft\internet explorer\dxtrans

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

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

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

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

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

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

explorer\main\featurecontrol\feature\_sslux

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

explorer\main\featurecontrol\feature\_sslux

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

settings\

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

Opens key:

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

settings\zonemap\

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

explorer\restrictions

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

f4ceaaf59cfc}

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

f4ceaaf59cfc}\treatas

 $\label{thm:continuous} Opens key: $$ HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas $$ Opens key: $$ HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas $$ HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas $$ HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas $$ HKCU\software\classes\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\treatas $$ HKCU\software\classes\wow6432node\clsid\software\clsid\softw$ 

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

f4ceaaf59cfc}\progid

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

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

f4ceaaf59cfc}\inprocserver32

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

f4ceaaf59cfc}\inprocserver32

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

f4ceaaf59cfc}\inprochandler32

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

f4ceaaf59cfc}\inprochandler32

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

f4ceaaf59cfc}\inprochandler

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

f4ceaaf59cfc}\inprochandler

Opens key: HKCU\software\policies\microsoft\internet explorer\control panel Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature\_iedde\_register\_urlecho

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

explorer\main\featurecontrol\feature\_iedde\_register\_urlecho

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

00aa00bbbb58}

Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}
Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\treatas

Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\progid

Opens key: HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-

00aa00bbbb58}\inprocserver32 HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-Opens key: 00aa00bbbb58}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-Opens key: 00aa00bbbb58}\inprochandler32 Opens key:  $HKCR \setminus wow6432 \\ node \setminus clsid \setminus \{f414c260-6ac0-11cf-b6d1-6ac0-11$ 00aa00bbbb58}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-Opens key: 00aa00bbbb58}\inprochandler HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-Opens key: 00aa00bbbb58}\inprochandler Opens key: HKLM\software\wow6432node\microsoft\windows script\features Opens key: HKLM\software\wow6432node\microsoft\com3 HKCU\software\classes\appid\1af5338669efabe0a9841478396871b1.exe Opens key: Opens key: HKCR\appid\1af5338669efabe0a9841478396871b1.exe Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat Opens key: HKLM\software\microsoft\ole\appcompat Opens key: HKLM\system\currentcontrolset\control\lsa Opens key: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy Opens kev: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration 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-c000-00000000046} Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32 Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32 Opens key: HKLM\system\currentcontrolset\services\bfe Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\recovery Opens key: HKLM\software\policies\microsoft\internet explorer\recovery HKCU\software\microsoft\internet explorer\recovery Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_scripturl\_mitigation HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_scripturl\_mitigation Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_block\_lmz\_img HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_block\_lmz\_img HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_behaviors HKLM\software\wow6432node\microsoft\internet Opens kev: explorer\main\featurecontrol\feature\_behaviors HKLM\software\wow6432node\microsoft\internet explorer\default behaviors Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid Opens key:  $HKCR\wow6432 node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\ \ progid$ Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32 HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-Opens key: 00aa00bdce0b}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandler  $HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-11cf-b$ Opens key: 00aa00bdce0b}\inprochandler Opens key: HKCU\software\policies\microsoft\internet explorer\persistence Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\persistence

Opens key: HKCU\software\policies\microsoft\internet explorer\persistence
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\persistence
Opens key: HKLM\software\wow6432node\policies\microsoft\internet
explorer\persistence
Opens key: HKLM\software\policies\microsoft\internet explorer\persistence
Opens key: HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas
Opens key: HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas
Opens key: HKCR\wow6432node\clsid\\81397204-f51a-4571-8d7b-dc030521aabd}\treatas

```
dc030521aabd}\progid
                                                                                 HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid
     Opens key:
     Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
                                                                                HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
     Opens kev:
dc030521aabd}\inprocserver32
     Opens key:
                                                                                 HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{81397204 - f51a - 4571 - 8d7b - f51a 
dc030521aabd}\inprochandler32
     Opens key:
                                                                                 HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler32
                                                                                HKCU\software\classes\wow6432node\clsid\{81397204-f51a-4571-8d7b-
     Opens kev:
dc030521aabd}\inprochandler
     Opens key:
                                                                                HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler
     Opens key:
                                                                                 HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{d1fe6762 - fc48 - 11d0 - 883a - fc48 - fc48 - 11d0 - 883a - fc48 
3c8b00c10000}
     Opens key:
                                                                                 HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
     Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\treatas
                                                                                 HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\treatas
     Opens key:
     Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\progid
                                                                                 HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid
     Opens kev:
     Opens key:
                                                                                 HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
     Opens key:
                                                                                 HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
     Opens key:
                                                                                 HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\progid
     Opens key:
                                                                                 HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\progid
                                                                                 HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
     Opens key:
3c8b00c10000}\inprocserver32
     Opens key:
                                                                                 HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32
                                                                                 HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{d1fe6762 - fc48 - 11d0 - 883a - 11d0 - 11d0
     Opens key:
3c8b00c10000}\inprochandler32
                                                                                 Opens key:
3c8b00c10000}\inprochandler32
                                                                                HKCU\software\classes\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
    Opens kev:
3c8b00c10000}\inprochandler
                                                                                 HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
     Opens key:
3c8b00c10000}\inprochandler
     Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}
                                                                                 HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
     Opens kev:
     Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\treatas
                                                                                 HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d\}\treatas
     Opens key:
     Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\progid
                                                                                 HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid
     Opens kev:
                                                                                 HKCU \setminus software \setminus classes \setminus clsid \setminus \{4fd2a832-86c8-11d0-8fca-00c04fd9189d\}
     Opens key:
     Opens key:
                                                                                 HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
                                                                                 HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
     Opens key:
```

00c04fd9189d}\progid

 Opens key:
 HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\progid

 Opens key:
 HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca

00c04fd9189d}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-

00c04fd9189d}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-

00c04fd9189d}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-

00c04fd9189d}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-

00c04fd9189d}\inprochandler

Opens key: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-

00c04fd9189d}\inprochandler

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

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

Opens key: HKLM\hardware\devicemap\video

Opens key: HKLM\system\currentcontrol\set\control\video\{43056cc8-3bf6-4ce7-bd67-

1e1a187c13e9}\0000

Opens key:

 $\label{local-bound} HKLM\system\currentcontrolset\enum\pci\ven_80ee\&dev\_beef\&subsys\_00000000\&rev\_00\3\&267a616a\&0\&10\\ Opens key: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-beef\&subsys\_00000000\&rev\_00\abella barbella bar$ 

9dd4432fa2e9}\0000

Opens key: HKLM\system\currentcontrolset\control\video\{42cf9257-1d96-4c9d-87f3-

0d8e74595f78}\0000

Opens key: HKLM\system\currentcontrolset\control\video\{b043b95c-5670-4f10-b934-

8ed0c8eb59a8}\0000

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility

Opens key:

Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug!

HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2 HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo Opens kev: Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3 HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98 Opens kev: Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue squadron Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder Opens kev: HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100 Opens key:  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus direct draw \setminus compatibility \setminus starcraft 115$ Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo HKLM\software\wow6432node\microsoft\directdraw\compatibilitv\terracide Opens kev: Opens key: HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension Opens key: Opens key: HKLM\software\wow6432node\microsoft\directdraw\gammacalibrator Opens key: HKLM\software\wow6432node\microsoft\directdraw Opens kev: HKLM\software\wow6432node\microsoft\direct3d Opens key: Opens key:  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \ nt \setminus current version \setminus msasn1$ Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231f941e9b7e1fe} HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe} Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-Opens kev: f941e9b7e1fe}\treatas  $HKCR\wow6432 node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\\treat as$ Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-Opens key: f941e9b7e1fe}\progid  $HKCR\wow6432node\clsid\a7ee7f34-3bd1-427f-9231-f941e9b7e1fe\\\progid$ Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-Opens kev: f941e9b7e1fe}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231f941e9b7e1fe}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231f941e9b7e1fe}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231f941e9b7e1fe}\inprochandler32 Opens key: HKCU\software\classes\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231f941e9b7e1fe}\inprochandler Opens key: HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231f941e9b7e1fe}\inprochandler HKCU\software\classes\dximagetransform.microsoft.shadow Opens kev: Opens key: HKCR\dximagetransform.microsoft.shadow Opens key: HKCU\software\classes\dximagetransform.microsoft.shadow\clsid Opens key: HKCR\dximagetransform.microsoft.shadow\clsid Opens key: 00c04fa34f05} HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05} Opens key: Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 12e34 + 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 12e34 + 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 12e34 + 12e34 + 12e34 + 12e34 \} \\ node \setminus clsid \setminus \{e71b4063 - 12e34 + 1$ 00c04fa34f05}\treatas HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\treatas Opens kev:

Opens key: 00c04fa34f05}\progid

HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid Opens key: Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e44 \} \\ + 12e44 + 12e44 + 12e44 \\ + 12e44 + 12e44 + 12e44 + 12e44 \\ + 12e44 + 12e44 + 12e44 + 12e44 + 12e44 + 12e44 + 1$ 

HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-

00c04fa34f05}\inprocserv er32

HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-Opens kev:

00c04fa34f05}\inprocserver32

 $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{e71b4063 - 3e59 - 11d2 - 952a - 12e34 \} \\ + 12e34 + 1$ Opens key:

00c04fa34f05}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-

00c04fa34f05}\inprochandler32

HKCU\software\classes\wow6432node\clsid\{e71b4063-3e59-11d2-952a-Opens kev:

00c04fa34f05}\inprochandler

Opens key: HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-

00c04fa34f05}\inprochandler

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

compatibility

Opens kev: HKLM\software\wow6432node\microsoft\internet explorer\activex

compatibility\{e71b4063-3e59-11d2-952a-00c04fa34f05}

Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db} HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db} Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-Opens key: 0000f87557db}\treatas Opens key:  $HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\$  \treatas HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-Opens key: 0000f87557db}\progid Opens key:  $HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid$ HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db} Opens key: Opens key: HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db} Opens key: HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\progid Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{4ch26c03-ff93-11d0-817e-0000f87557db}\inprocserver32 Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{4cb26c03 - ff93 - 11d0 - 817e - 12d0 - 12d0$ 0000f87557db}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-Opens kev: 0000f87557db}\inprochandler Opens key: HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler Opens key: f4fc1e6ca1bd} Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd} Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6f4fc1e6ca1bd}\treatas HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6f4fc1e6ca1bd}\progid  $HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid$ Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6f4fc1e6ca1bd}\inprocserver32 HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-Opens key: f4fc1e6ca1bd}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-Opens key: f4fc1e6ca1bd}\inprochandler32 HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-Opens key: f4fc1e6ca1bd}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-Opens key: f4fc1e6ca1bd}\inprochandler Opens key: HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6f4fc1e6ca1bd}\inprochandler Opens key: HKCU\software\classes\typelib HKCR\typelib Opens key:  $HKCU \setminus software \setminus classes \setminus typelib \setminus \{5e77eb03-937c-11d1-b047-00aa003b6061\}$ Opens key: Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061} HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1 Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1 Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-Opens key: 00aa003b6061}\1.1\409 HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409 Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-Opens key: 00aa003b6061}\1.1\9 HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9 Opens key: Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0 Opens key: HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0 Opens key: HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32 HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32 Opens key: Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db} Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}  $HKCU \setminus software \\ \\ classes \\ \\ typelib \\ \\ \{54314d1d-35fe-11d1-81a1-0000f87557db\} \\ \\ 1.1 \\ \\ 1.2 \\ \\ 1.3 \\ \\ 1.4 \\$ Opens key: Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1 Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\409 HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\409 Opens kev: Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\9 Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\9 Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0 HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0 Opens kev: Opens key: HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32 Opens key: HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_disable\_behaviors\_draw\_reentrancy

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature disable behaviors draw reentrancy Opens key: 00aa003f8646} Opens kev: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646} Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{275c23e2-3747-11d0-9fea-18432 \\ node \setminus clsid \setminus \{275c23e2-3747-11d0-9fea-18422 \\ node \setminus clsid \setminus \{275c23e2-37442 \\ node \setminus \{275c23e2-37442 \\ nod$ 00aa003f8646}\treatas HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\treatas Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid Opens kev: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid Opens key:  $HKCU \setminus software \setminus classes \setminus clsid \setminus \{275c23e2-3747-11d0-9fea-00aa003f8646\}$ Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646} Opens key: HKCU\software\classes\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid Opens key: HKCR\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\progid Opens kev: HKCU\software\classes\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprocserver32 Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{275c23e2-3747-11d0-9fea-1484\} \\ + \{275c23e2-3747-11d0-9fea-1484\}$ 00aa003f8646}\inprochandler32 HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-Opens kev: 00aa003f8646}\inprochandler32 Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{275c23e2-3747-11d0-9fea-1864\} \\ + 11d0-9fea-1864 \\$ 00aa003f8646}\inprochandler Opens key: HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}\inprochandler HKCU\software\microsoft\internet explorer\international\scripts\26 Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\simsun HKLM\system\currentcontrolset\services\netbt\linkage Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_binary\_caller\_service\_provider HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_binary\_caller\_service\_provider Opens key: HKCU\software\classes\wow6432node\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32 HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-Opens key: 00aa00389b71}\proxystubclsid32 Opens key: HKCU\software\classes\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119} HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-00c04fd90119} Opens kev: Opens key: 00c04fd90119}\proxystubclsid32 HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-Opens key: 00c04fd90119}\proxystubclsid32 Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-000000000046} HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\treatas Opens key: Opens key: 000000000046}\progid  $HKCR\wow6432 node\\clsid\\\{00020424-0000-0000-c000-000000000046\\\}\\\progid$ Opens key: Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-00000000046} Opens key: HKCR\clsid\{00020424-0000-0000-c000-00000000046}  $\label{local-eq:hkcu-software-classes-clsid-software-classes-clsid-software-coordinates} HKCU \setminus software \setminus classes \setminus clsid \setminus \{00020424-0000-0000-c000-c000-c000-c000-c0000-c00-c000-c000-c0$ Opens key: 000000000046}\progid Opens key: HKCR\clsid\{00020424-0000-0000-c000-00000000046}\progid Opens key: 000000000046}\inprocserv er32 Opens key: HKCR\wow6432node\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-Opens kev: 00000000046}\inprochandler32 HKCR\wow6432node\clsid\{00020424-0000-0000-c000-Opens key: 000000000046}\inprochandler32 Opens kev: HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-00000000046}\inprochandler HKCR\wow6432node\clsid\{00020424-0000-0000-c000-Opens kev:

000000000046}\inprochandler

HKCU\software\classes\mime\database\content type\image/png

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

Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}

HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01} Opens key: Opens key: HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas

Opens key:  $HKCR \setminus wow6432 node \\ clsid \\ \{30c3b080-30fb-11d0-b724-00aa006c1a01\} \\ \setminus treatas$ HKCU\software\classes\wow6432node\clsid\{30c3b080-30fb-11d0-b724-Opens key:

00aa006c1a01}\progid

Opens key:  $HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\progid$ Opens key: 00aa006c1a01}\inprocserver32 HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-Opens key: 00aa006c1a01}\inprocserver32 Opens key: 00aa006c1a01}\inprochandler32 HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-Opens key: 00aa006c1a01}\inprochandler32 Opens key: 00aa006c1a01}\inprochandler Opens key: HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01} Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01} Opens kev: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas Opens key:  $HKCR\wow6432 node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\treatas$ Opens key: HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid Opens key: 00aa006c1a01}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32 Opens key: 00aa006c1a01}\inprochandler32 HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-Opens key: 00aa006c1a01}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{6a01fda0-30df-11d0-b724-Opens kev: 00aa006c1a01}\inprochandler HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-Opens key: 00aa006c1a01}\inprochandler Opens key: HKCU\software\classes\mime\database\content type Opens key: HKCR\mime\database\content type Opens key: HKCU\software\classes\mime\database\content type\image/bmp\bits Opens key: HKCR\mime\database\content type\image/bmp\bits Opens key: HKCU\software\classes\mime\database\content type\image/gif\bits Opens key: HKCR\mime\database\content type\image/gif\bits Opens key: HKCU\software\classes\mime\database\content type\image/jpeg\bits Opens key: HKCR\mime\database\content type\image/jpeg\bits HKCU\software\classes\mime\database\content type\image/pjpeg\bits Opens kev: Opens key: HKCR\mime\database\content type\image/pjpeg\bits Opens key: HKCU\software\classes\mime\database\content type\image/png\bits Opens key: HKCR\mime\database\content type\image/png\bits Opens key:  $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \slight \mbox{tiff} \label{lem:hkcu} \\ \end{tabular}$ Opens key: HKCR\mime\database\content type\image/tiff\bits Opens kev: HKCU\software\classes\mime\database\content type\image/x-icon\bits Opens key: HKCR\mime\database\content type\image/x-icon\bits Opens key: HKCU\software\classes\mime\database\content type\image/x-jg\bits Opens key: HKCR\mime\database\content type\image/x-jg\bits Opens key: HKCU\software\classes\mime\database\content type\image/x-png\bits Opens key: HKCR\mime\database\content type\image/x-png\bits Opens kev: HKCU\software\classes\mime\database\content type\image/x-wmf\bits Opens key: HKCR\mime\database\content type\image/x-wmf\bits Opens key: HKCU\software\classes\mime\database\content type\image/x-png Opens key: HKCR\mime\database\content type\image/x-png Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750} Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750} Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{a3ccedf7-2de2-11d0-86f4-12de2-11d0-86$ 00a0c913f750}\treatas HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas Opens kev: Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserv er32 HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-Opens kev: 00a0c913f750}\inprocserver32  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{a3ccedf7-2de2-11d0-86f4-12de2-1$ Opens kev: 00a0c913f750}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-Opens kev: 00a0c913f750}\inprochandler Opens key: HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_activex\_inactivate\_mode\_removal\_revert

HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol\feature\_activex\_inactivate\_mode\_removal\_revert

Opens key: HKCU\software\classes\mime\database\content type\application/javascript

Opens key: HKCR\mime\database\content type\application/javascript

Opens key: HKCU\software\microsoft\internet

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

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

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

explorer\main\featurecontrol\feature\_block\_lmz\_script

Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}

Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\treatas

00c04fb6bfc4}\progid

 $\label{thm:continuous} Opens~key: $$ HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid $$ Opens~key: $$ HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}$$$ 

00c04fb6bfc4}\progid

Opens key:  $\label{limits} \mbox{HKCR\clsid\f7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\progid$ 

Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprochandler

Opens key: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-

00c04fb6bfc4}\inprochandler

Opens key: HKCU\software\microsoft\internet explorer\feed discovery

Opens key: HKLM\software\wow6432node\microsoft\internet explorer\feed discovery

Opens key: HKCU\software\microsoft\ftp

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

fd2b31b3eefd}

fd2b31b3eefd}\treatas

fd2b31b3eefd}\progid

Opens key:  $\begin{tabular}{ll} HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\progid\\ Opens key: \\ HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\end{tabular}$ 

fd2b31b3eefd}\progid

Opens key:  $\label{lem:hkcrlsid} \begin{tabular}{ll} HKCR\clsid\e569bde7-a8dc-47f3-893f-fd2b31b3eefd\progid \\ \end{tabular}$ 

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

fd2b31b3eefd}\inprocserver32

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

fd2b31b3eefd}\inprocserver32

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

fd2b31b3eefd}\inprochandler32

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

fd2b31b3eefd}\inprochandler32

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

fd2b31b3eefd}\inprochandler

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

fd2b31b3eefd}\inprochandler

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

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

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

Opens key: HKLM\software\policies\microsoft\internet explorer\services
Opens key: HKCU\software\microsoft\internet explorer\services
Opens key: HKLM\software\wow6432node\policies\microsoft\internet

Opens key: explorer\activities

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

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

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

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

explorer\infodelivery\restrictions

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

explorer\infodelivery\restrictions

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

explorer\infodelivery\restrictions

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

sites

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

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

08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-

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

Opens key:

a2d8-08002b30309d}\shellfolder

Opens key:

 $\label{thm:condition} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \end{tabular} \label{thm:condition}$ 

Opens key:

11e3-a68e-806e6f6e6963}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

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

b8dc300d9f9d}

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

b8dc300d9f9d}\treatas

Opens key:  $\begin{tabular}{ll} HKCR\wow6432node\clsid\f1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\treatas \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\f1f486a52-3cb1-48fd-8f50-\\ \end{tabular}$ 

b8dc300d9f9d}\progid

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

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

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

b8dc300d9f9d}\progid

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

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

 $b8dc300d9f9d\\ \\ \\ inprochandler$ 

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

Opens key:

11e3-a68e-806e6f6e6963}\

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ shell registered applications \ variations \ directory \ open with progids \ microsoft \ windows \ shell \ registered \ microsoft \ microsoft \ windows \ shell \ registered \ microsoft \ microso$ 

Opens key:

HKCU\software\microsoft\windows\shell\associations\urlassociations\directory

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

Opens key: HKCU\software\classes\directory\curver

Opens key: HKCR\directory\curver
Opens key: HKCR\directory\

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

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

Opens key: HKCR\folder

Opens key:  $\label{lem:hkcusoftware} \mbox{Liconhandler} \mbox{ HKCU\software\classes\folder\shellex\liconhandler} \mbox{}$ 

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

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

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

Opens key: HKCR\directory\docobject

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

Opens key: HKCR\folder\docobject

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

Opens key: HKCR\allfilesystemobjects\docobject

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

Opens key: HKCR\directory\browseinplace

```
HKCU\software\classes\folder\browseinplace
      Opens key:
      Opens key:
                                                                                  HKCR\folder\browseinplace
      Opens kev:
                                                                                  HKCU\software\classes\allfilesystemobjects\browseinplace
      Opens key:
                                                                                  HKCR\allfilesystemobjects\browseinplace
      Opens key:
                                                                                  HKCU\software\classes\directory\clsid
      Opens key:
                                                                                  HKCR\directory\clsid
      Opens key:
                                                                                  HKCU\software\classes\folder\clsid
      Opens key:
                                                                                  HKCR\folder\clsid
      Opens key:
                                                                                  HKCU\software\classes\allfilesystemobjects\clsid
                                                                                  HKCR\allfilesystemobjects\clsid
      Opens key:
      Opens key:
                                                                                  HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c2a7 - c2a7
444553540000}
      Opens key:
                                                                                  HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
                                                                                  HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c2a7 - c2a7
      Opens key:
444553540000}\inprocserver32
      Opens key:
                                                                                  HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32
      Opens key:
                                                                                  HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
 444553540000}\shellfolder
      Opens key:
                                                                                 HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\shellfolder
      Opens key:
                                                                                  HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\treatas
      Opens key:
                                                                                  HKCR\wow6432node\clsid\ff393560-c2a7-11cf-bff4-444553540000\treatas
      Opens key:
                                                                                  HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c2a7 - 
444553540000}\progid
      Opens key:
                                                                                  HKCR\wow6432 node\\clsid\\\{ff393560-c2a7-11cf-bff4-444553540000\}\\\progid
      Opens key:
                                                                                  HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
                                                                                  HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}
      Opens key:
      Opens key:
                                                                                  HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\progid
                                                                                  HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\progid
      Opens key:
      Opens key:
                                                                                  HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{ff393560 - c2a7 - 11cf - bff4 - c2a7 - c2a7
444553540000}\inprochandler32
                                                                                 Opens key:
 444553540000}\inprochandler32
     Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprochandler
                                                                                  HKCR\wow6432node\clsid\ff393560-c2a7-11cf-bff4-
      Opens key:
444553540000}\inprochandler
      Opens key:
c2a7-11cf-bff4-444553540000}
                                                                                 HKCU\software\microsoft\windows\currentversion\internet
      Opens key:
 settings\5.0\cache\extensible cache\mshist012016042220160423
                                                                                 HKCU\software\microsoft\windows\currentversion\app
      Opens key:
paths\1af5338669efabe0a9841478396871b1.exe
      Opens key:
                                                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\1af5338669efabe0a9841478396871b1.exe
     Opens key:
                                                                                 HKLM\software\microsoft\windows\currentversion\app
paths\1af5338669efabe0a9841478396871b1.exe
                                                                                 HKCU \setminus software \setminus icrosoft \setminus windows \setminus current version \setminus explorer \setminus (20d04feo-block) + 
      Opens kev:
3aea-1069-a2d8-08002b30309d}
      Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in fo \ 1 \ desktop \ name space \ name \ customizations
      Opens key:
                                                                                 HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 08002b30309d}
      Opens key:
                                                                                  HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
                                                                                  HKCU\software\microsoft\internet explorer\main\windowssearch
      Opens key:
      Opens key:
                                                                                  HKLM\software\policies\microsoft\internet explorer\feeds
      Opens key:
                                                                                  HKCU\software\microsoft\internet explorer\feeds
      Opens key:
                                                                                  HKLM\software\wow6432node\microsoft\internet explorer\feeds
      Opens key:
68ad-4d8a-87bd-30b759fa33dd}
68 ad-4d8 a-87 bd-30 b759 fa 33 dd \} \verb|\property| bag
      Opens key:
                                                                                  HKLM\software\wow6432node\microsoft\windows search
      Opens kev:
                                                                                  HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
                                                                                  HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
      Opens kev:
      Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
      Opens key:
                                                                                  HKCU\software\classes\mime\database\content type\image/x-icon
      Opens kev:
                                                                                  HKCR\mime\database\content type\image/x-icon
      Opens key:
                                                                                  HKCU\software\classes\protocols\filter\image/x-icon
                                                                                  HKCR\protocols\filter\image/x-icon
      Opens kev:
      Opens key:
                                                                                 HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
      Opens key:
                                                                                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_treat_image_as_authoritative
      Queries value:
                                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options[disableusermodecallbackfilter]
                           HKLM\system\currentcontrolset\control\session
  Oueries value:
manager[cwdillegalindllsearch]
  Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Oueries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Queries value:
                           HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  Oueries value:
                           HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
  Queries value:
                           HKCU\control panel\desktop[preferreduilanguages]
  Oueries value:
                           HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [preferex ternal manifest]] \ details a software \ wow 6432 node \ microsoft \ windows \ current \ version \ side by side \ preferex \ ternal \ manifest]
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                           HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Oueries value:
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                           HKLM\software\wow6432node\microsoft\windows
  Queries value:
nt\currentversion\compatibility32[1af5338669efabe0a9841478396871b1]
                           HKLM\software\wow6432node\microsoft\windows
  Queries value:
nt\currentversion\windows[loadappinit dlls]
  Queries value:
                           HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:
                           HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
                           HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Oueries value:
  Queries value:
                           HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[disableimprovedzonecheck]
                           HKLM\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[security_hklm_only]
                           HKLM\software\wow6432node\microsoft\windows\windows error
  Oueries value:
reporting\wmr[disable]
                           HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:
  Queries value:
                           HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Oueries value:
                           HKLM\system\currentcontrolset\control\nls\locale[00000409]
                           HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:
                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
                           HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
                           HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value:
                           HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane11]|
                           HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
                           HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane14]|
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value:
                           HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
                           HKLM\system\currentcontrolset\control\cmf\config[system]
  Oueries value:
  Queries value:
                           HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui]
  Oueries value:
                           HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg]
  Oueries value:
                           HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Oueries value:
                           HKLM\software\microsoft\com3[com+enabled]
  Oueries value:
                           HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]
  Queries value:
                           HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
  Oueries value:
                           HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
```

```
Queries value:
                                     HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[]
  Oueries value:
                                     HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
                                     HKLM\software\microsoft\ole[maxsxshashcount]
  Oueries value:
  Queries value:
                                     HKLM\software\microsoft\rpc[maxrpcsize]
  Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:
                                     HKLM\system\setup[oobeinprogress]
  Queries value:
                                     HKLM\system\setup[systemsetupinprogress]
                                     HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Oueries value:
  Queries value:
                                     HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Oueries value:
                                     HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Queries value:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings[createuricachesize]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[createuricachesize]
                                     Queries value:
settings[createuricachesize]
  Oueries value:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Queries value:
settings[enablepunycode]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[enablepunycode]
                                     HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_http_username_password_disable[1af5338669efabe0a9841478396871b1.exe]
                                     HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_http_username_password_disable[*]
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
                                     HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Oueries value:
                                     HKLM \verb|\system| current controlset \verb|\services|| ldap[use old host resolution order]
  Queries value:
                                     HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
  Oueries value:
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
                                     HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
  Queries value:
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
                                     HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main[frametabwindow]
                                     HKCU\software\microsoft\internet explorer\main[framemerging]
  Oueries value:
                                     HKLM\software\wow6432node\microsoft\internet explorer\main[framemerging]
  Queries value:
  Queries value:
                                     HKCU\software\microsoft\internet explorer\main[sessionmerging]
                                     HKLM\software\wow6432node\microsoft\internet
  Queries value:
explorer\main[sessionmerging]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\main[admintabprocs]
                                     HKLM\software\wow6432node\microsoft\internet
  Oueries value:
explorer\main[admintabprocs]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
  Queries value:
                                     HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| internet
explorer\main[tabprocgrowth]
  Queries value:
                                     HKLM\software\wow6432node\microsoft\internet
explorer\main[navigationdelay]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[attributes]
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[callforattributes]
  Queries value:
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[restrictedattributes]
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[wantsfordisplay]
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
  Oueries value:
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[usedrophandler]
                                     HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
```

Oueries value:

08002b30309d}\shellfolder[wantsforparsing]

```
HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                                                 HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[queryforoverlay]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[queryforinfotip]
                                                 HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[hideinwebview]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
   Oueries value:
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsaliasednotifications]
   Oueries value:
                                                 HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\shellfolder[nofilefolderjunction]
   Queries value:
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[pintonamespacetree]
                                                 HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\shellfolder[hasnavigationenum]
                                                Queries value:
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
   Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ monenum \ [\{871c5380-42a0-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1069-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea-1060-a2ea
08002b30309d}]
   Queries value:
                                                 HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\inprocserver32[loadwithoutcom]
                                                HKCU\software\microsoft\windows\currentversion\shell
   Queries value:
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0xffff]
   Oueries value:
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Queries value:
08002b30309d}\inprocserver32[inprocserver32]
                                                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\inprocserver32[threadingmodel]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nofilemenu]
                                                 HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[urlencoding]
                                                 HKLM\software\wow6432node\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_unc_savedfilecheck[1af5338669efabe0a9841478396871b1.exe]
   Queries value:
                                                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
   Oueries value:
                                                HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\0[flags]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\2[flags]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
                                                 \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
   Queries value:
settings\zones\4[flags]
   Queries value:
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[1af5338669efabe0a9841478396871b1.exe]
                                                HKCU\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                                                HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[1af5338669efabe0a9841478396871b1.exe]
                                                HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
   Queries value:
                                                HKLM\system\currentcontrolset\control\wmi\security[Ocfe0455-93ba-440d-
a3fe-553973d0b723]
   Queries value:
                                                 HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce4]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[fromcachetimeout]
   Queries value:
                                                 \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings[secureprotocols]
   Queries value:
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
                                                 HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[secureprotocols]
   Queries value:
                                                \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} internet \\ \end{tabular}
settings[certificaterevocation]
   Queries value:
                                                 \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
```

```
settings[disablekeepalive]
   Oueries value:
                                                       HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
    Queries value:
                                                       HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
    Queries value:
                                                       HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
                                                       HKLM\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[enablehttp1_1]
    Queries value:
                                                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
    Queries value:
                                                       HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
   Queries value:
                                                       HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                                                       HKCU\software\policies\microsoft\windows\currentversion\internet
    Queries value:
settings[proxyhttp1.1]
    Queries value:
                                                       HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                                                       HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[enablenegotiate]
                                                       HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[disablebasicoverclearchannel]
                                                       HKCU\software\microsoft\internet
    Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                                      HKLM\software\wow6432node\microsoft\internet
    Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                                      HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[clientauthbuiltinui]
                                                       HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[syncmode5]
                                                      HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet
    Queries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                                                      HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings\5.0\cache[signature]
                                                      HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings\5.0\cache\content[peruseritem]
                                                      HKLM\software\wow6432node\microsoft\windows\currentversion\internet
    Queries value:
settings\5.0\cache\content[peruseritem]
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-16444, \ node \ 
33be-4251-ba85-6007caedcf9d}[category]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[name]
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (352481e8-1648) \ microsoft \ windows \ current \ version \ (352481e8-1648) \ microsoft \ windows \ current \ version \ (352481e8-1648) \ microsoft \ windows \ current \ version \ (352481e8-1648) \ microsoft \ windows \ current \ version \ (352481e8-1648) \ microsoft \ windows \ current \ version \ (352481e8-1648) \ microsoft \ windows \ current \ windows \ microsoft \ windows \ windows \ microsoft \ windows \ microsoft \ windows \ windows \ microsoft \ windows \ 
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]
   Queries value:
33be-4251-ba85-6007caedcf9d}[localizedname]
    Oueries value:
33be-4251-ba85-6007caedcf9d}[icon]
    Queries value:
HKLM \label{lem:hklm} White the software \label{lklm} White the 
33be-4251-ba85-6007caedcf9d}[security]
    Oueries value:
33be-4251-ba85-6007caedcf9d}[streamresource]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[streamresourcetype]
    Oueries value:
33be-4251-ba85-6007caedcf9d}[localredirectonly]
   Oueries value:
33be-4251-ba85-6007caedcf9d}[roamable]
    Oueries value:
```

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

Queries value:

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

Queries value:

 $\label{thm:local-basic$ 

Oueries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 caedcf9d\} \ [folder type id]$ 

Oueries value:

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

Queries value:

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

folders[cache]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

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

Queries value:

 $\label{thm:local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\ff1b32785-65ba-4fcf-9d55-7b8e7f157091\}[security]$ 

Queries value:

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

Queries value:

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

Queries value:

 $\label{localization} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fiba-4fcf-9d55-7b8e7f157091 \fill \current \current$ 

Queries value:

 $\label{thm:local-bound} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fifthgar785-6fba-4fcf-9d55-7b8e7f157091\firsymmetric{1}{1} [roamable]$ 

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{fiba} $$Hklm \end{fiba} $$Hklm \end{fiba} $$ \end{fi$ 

Queries value:

Queries value:

 $\label{thm:hammon} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \fiba-4fcf-9d55-7b8e7f157091 \end{substitute} a tributes \footnote{Thm:hammon-ha$ 

Queries value:

Queries value:

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

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

folders[local appdata]

Queries value:

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

Oueries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[infotip]} Infotip in the property of the property of$ 

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[publishexpandedpath]}$ 

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[foldertypeid]}$ 

Queries value:

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

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

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

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

settings\5.0\cache\cookies[peruseritem]

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{align*.} Hklm \end{align*.} Which is a substitution and the substitution of th$ 

Queries value:

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

Queries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cdot 2b0 f765 d-c0e9-4171-908e-08a611b84 ff6 \cdot [parent folder]$ 

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \coe9-4171-908e-08a611b84ff6 \cite{linfotip} \end{subarray} in factor \cite{linfotip} \end{subarray} % \label{thm:local-ham}$ 

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

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

Oueries value

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

Oueries value:

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

Ougrige value.

 $\label{local-ham} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \current \cu$ 

Queries value

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

Oueries value

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

Oueries value:

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

Queries value:

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

Queries value: folders[cookies]

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

Oueries value

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value

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

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

folders[appdata]

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

settings\5.0\cache\cookies[cacheprefix]

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

settings\5.0\cache\cookies[cachelimit]

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

settings\5.0\cache\history[peruseritem]

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

settings\5.0\cache\history[peruseritem]

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \end{d} 9dc 8a3bb784-432e-a781-5a1130a75963 \[info tip]$ 

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{align*.} Hklm \end{align*.} Hklk \end{align*.} Which is a simple to the soft windows \end{align*.} Hklk \end{align*.} Which is a simple to the soft \end{align*.} Hklk \end{al$ 

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder b784-432e-a781-5a1130a75963\folder b784-432e-a781-5a110a75963\folder b784-432e-a781-5a110a75963\folder b784-$ 

Oueries value:

 $HKLM \coftware \wow6432 node \mbox{$microsoft\windows\currentversion\explorer\folder descriptions\{$d9dc8a3b-b784-432e-a781-5a1130a75963\}[precreate]}$ 

Queries value:

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

Queries value:

 $\label{thm:local_explorer_local_ex$ 

```
b784-432e-a781-5a1130a75963}[publishexpandedpath]
 Oueries value:
b784-432e-a781-5a1130a75963}[attributes]
 Oueries value:
b784-432e-a781-5a1130a75963}[foldertypeid]
 Oueries value:
b784-432e-a781-5a1130a75963}[initfolderhandler]
                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[history]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[cachelimit]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
 Queries value:
                         \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\5.0\cache\extensible cache\ietld[cacherepair]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
 Queries value:
                         \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \\
settings\5.0\cache\extensible cache\privacie:[cachepath]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[enableautoproxyresultcache]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
 Queries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[mbcsapiforcrack]
 Queries value:
                         \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings[utf8servernameres]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                         Oueries value:
settings[disableworkerthreadhibernation]
 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}.
```

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

settings[disablereadrange]

Queries value:

```
settings[socketsendbufferlength]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[socketreceivebufferlength]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperproxv]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[connecttimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[sendtimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablentlmpreauth]
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Queries value:
settings[scavengecachelowerbound]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelifetime]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[ftpdefaultexpirytimesecs]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback[1af5338669efabe0a9841478396871b1.exe]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[perusercookies]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[leashlegacycookies]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[wpadsearchalldomains]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocachecheck]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
```

```
Oueries 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:
                                                                 settings[sharecredswithwinhttp]
                                                                 HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[mimeexclusionlistforcache]
                                                                 HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[headerexclusionlistforcache]
                                                                 HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[dnscacheenabled]
                                                                 \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma of the 
    Queries value:
settings[dnscacheentries]
                                                                 HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[dnscachetimeout]
                                                                 HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[warnonpost]
                                                                 \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma of the 
    Queries value:
settings[warnalwaysonpost]
                                                                 HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[warnonzonecrossing]
                                                                 HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[warnonbadcertrecving]
                                                                 HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[warnonpostredirect]
                                                                 \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
    Queries value:
settings[alwaysdrainonredirect]
                                                                 HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[warnonhttpstohttpredirect]
    Queries value:
                                                                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
    Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
    Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
    Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 00000000001[library path]) \ (library path) \ (library path
    Queries 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]
    Queries 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]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
    Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ (0000000000001[version]) \ details \ det
```

Queries 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\0000000000002[displaystring]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[supportednamespace]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ catalog\_entries \ 0000000000003 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid] Queries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \names pace\_catalog 5 \catalog\_entries \names family] \\ Queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
   Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[version]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[storesserviceclassinfo]
  Queries value:
- $\label{lem:hklmsystem} Hklm\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerinfo]\queries\value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[enabled]
  Queries value:
- $\label{lem:hklm} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version]\\ Oueries\ value: \begin{tabular}{ll} Color of the color of$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
- 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:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version]
- $\label{local-parameters} HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000005[storesserviceclassinfo]\ Queries\ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[librarypath]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerid]
  Oueries value:

Oueries value:  $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000006 [supported name space]]$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[enabled] Oueries value: Oueries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 10000000000006 \ [storesservice class in fo]$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[providerinfo] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32numhandlebuckets] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\wpad[wpadoverride]  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma of the$ Queries value: settings[enableautodial] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[nonetautodial] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[globaluseroffline] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[badproxyexpirestime] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[disablebranchcache] HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing] Queries value: Queries value:  $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 1af 5338669 ef abe 0a 9841478396871b1\_rasapi 32[enable file tracing]$ Queries value:  $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 1af5338669 efabe 0a9841478396871b1\_rasapi32[file tracing mask]$ HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasapi32[enableconsoletracing] Queries value:  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 1af5338669 efabe 0a9841478396871b1\_rasapi32[consoletracing mask]$ Queries value:  $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 1af5338669 efabe 0a9841478396871b1\_rasapi32 \ [maxfilesize]$ HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasapi32[filedirectory] Queries value:  $HKLM \label{lem:hklm} White the label{lem:hklm} HKLM \label{lem:hklm} White the label{lem:hkklm} HKLM \label{lem:hkklm} White the label{lem:hkklm} HKLM \label{lem:hkklm} White the label{lem:hkklm} White the label{lem:hkklm} White the label{lem:hkklm} White the label{lem:hkklm} HKLM \label{lem:hkklm} White the label{lem:hkklm} White the label{lem:hkkl$ Queries value:  $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 1af 5338669 efabe 0a 9841478396871b1\_rasmancs [file tracing mask]$ HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasmancs[enableconsoletracing] Queries value:  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus 1af5338669 efabe 0a9841478396871b1\_rasmancs[consoletracing mask]$ Queries value:  $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 1af5338669e fabe 0a9841478396871b1\_rasmancs \ [maxfilesize]$ Queries value: HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1 rasmancs[filedirectorv] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[programdata]  $HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled processes \texttt{[a5ea4f8e]}$ Oueries value: Queries value: HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling] Oueries value: HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession] Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[proxysettingsperuser] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[migrateproxy] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[proxyserver] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[proxyoverride] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\connections[savedlegacysettings] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Queries value:  $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}$ settings\zonemap[autodetect] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value:

 $\label{lem:hklmsystem} HKLM \xspace \xspace$ 

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

Queries value:

```
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
   Oueries 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]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
   Queries value:
                                                 HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
   Oueries value:
                                                 HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
   Oueries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} set \end{tabular} and \end{tabular} is a simular \end{tabular} and \end{tabular} system \end{tabular} control set \end{tabular} set \end{tabular} is a simular \end{tabular} is a simular \end{tabular} set \end{tabu
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable dynamic update]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[registerprimarvname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
   Queries value:
HKLM \verb| system| current control set \verb| services| tcpip| parameters[enable adapter domain name registration]| to the first of the firs
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetop]eveldomainzones]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
   Oueries value:
                                                 HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
                                                 HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
   Oueries value:
   Oueries value:
Oueries value:
```

```
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [enable multicast]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
                         HKCU\software\microsoft\internet explorer[no3dborder]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet explorer[no3dborder]
 Queries value:
 Queries value:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings[urlencoding]
                         \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[urlencoding]
                         HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_mime_handling[1af5338669efabe0a9841478396871b1.exe]
                         HKLM\software\wow6432node\microsoft\internet
 Queries value:
\verb|explorer\main\featurecontrol\feature\_mime\_handling[*]|
                         \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
 Queries value:
settings\5.0\user agent[]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\user agent[]
                         HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\user agent[compatible]
                         Queries value:
settings\5.0\user agent[compatible]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[version]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet settings[user
agent]
 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]
                         HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_browser_emulation[1af5338669efabe0a9841478396871b1.exe]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
                         HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_maxconnectionsperserver[1af5338669efabe0a9841478396871b1.exe]
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserver[*]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver[1af5338669efabe0a9841478396871b1.exe]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_0server[*]
                         HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
 Queries value:
                         HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
                         HKLM\system\currentcontrolset\services\winsock\setup
 Oueries value:
migration\providers\tcpip[winsock 2.0 provider id]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [used elayed acceptance]
```

```
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
 Oueries value:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableutf8]
                         HKCU\software\microsoft\internet explorer\international[acceptlanguage]
 Oueries value:
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression[1af5338669efabe0a9841478396871b1.exe]
                         HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_disable_legacy_compression[*]
 Oueries value:
HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]|
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
 Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\autosuggestl
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
 Queries value:
                         HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[]
                         HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
 Oueries value:
00c04fd7d062}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
 Queries value:
00c04fd7d062}\inprocserver32[]
                         HKCR\wow6432node\clsid\{00bb2765-6a77-11d0-a535-
 Queries value:
00c04fd7d062}\inprocserver32[threadingmodel]
                         HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-9fe3c77a297a}[]
 Oueries value:
                         HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
 Queries value:
9fe3c77a297a}\inprocserver32[inprocserver32]
                        HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
 Queries value:
9fe3c77a297a}\inprocserver32[]
 Queries value:
                         HKCR\wow6432node\clsid\{6935db93-21e8-4ccc-beb9-
9fe3c77a297a}\inprocserver32[threadingmodel]
                         HKCU\software\microsoft\windows\currentversion\explorer\runmru[mrulist]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\runmru[a]
 Oueries value:
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\runmru[d]
                         HKCU\software\microsoft\windows\currentversion\explorer\runmru[c]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\runmru[b]
 Queries value:
 Queries value:
                         HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-00c04fd7d062}[]
                         HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
 Queries value:
00c04fd7d062}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
 Queries value:
00c04fd7d062}\inprocserver32[]
                         HKCR\wow6432node\clsid\{00bb2764-6a77-11d0-a535-
 Queries value:
00c04fd7d062}\inprocserver32[threadingmodel]
 Queries value:
                         HKCR \wow6432 node \clsid \ \{00bb2763-6a77-11d0-a535-00c04fd7d062\}[]
                         HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
 Oueries value:
00c04fd7d062}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
 Oueries value:
00c04fd7d062}\inprocserver32[]
 Queries value:
                         HKCR\wow6432node\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
                         HKCR\wow6432node\clsid\{03c036f1-a186-11d0-824a-
 Oueries value:
00aa005b4383}\inprocserver32[]
 Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\autocomplete\client[]
                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}\progid[]
 Oueries value:
                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-b61bb7cdd997}[]
 Queries value:
 Queries value:
                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
b61bb7cdd997}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
 Queries value:
b61bb7cdd997}\inprocserver32[]
                         HKCR\wow6432node\clsid\{807c1e6c-1d00-453f-b920-
 Queries value:
b61bb7cdd997}\inprocserver32[threadingmodel]
 Queries value:
                         HKLM\software\microsoft\rpc\extensions[ndroleextdll]
 Oueries value:
                         HKCU\control panel\desktop[smoothscroll]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
 Queries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[acclistviewv6]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
                         \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings\zones\3[1a10]
 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\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]

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

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[searchlist]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpv6domain]

e1e01c1f69b5}[nameserver]

Queries value:

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

Queries value:

e1e01c1f69b5}[dhcpnameserver]

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

Oueries value:

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

Queries value:

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

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

Queries value:

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

Oueries value:

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

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

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

Oueries value:

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

Queries value:

e1e01c1f69b5}[disableadapterdomainname]

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

```
806e6f6e6963}[disableadapterdomainname]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[disabledynamicupdate]
 Oueries value:
806e6f6e6963}[enableadapterdomainnameregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registrationmaxaddresscount]
 Oueries value:
806e6f6e6963}[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enablemulticast]
                        HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
 Queries value:
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
                        HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[privacyadvanced]
                        HKCR\mime\database\content type\text/html[extension]
 Queries value:
                        HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_mime_sniffing[1af5338669efabe0a9841478396871b1.exe]
                        HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_mime_sniffing[*]
                        HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[istextplainhonored]
                        HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_feeds[1af5338669efabe0a9841478396871b1.exe]
                        HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_feeds[*]
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[1af5338669efabe0a9841478396871b1.exe]
 Oueries value:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
                        HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
 Oueries value:
                        HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[]
 Oueries value:
                        HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
 Queries value:
00aa00686f13}\inprocserver32[inprocserver32]
                        HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
 Oueries value:
00aa00686f13}\inprocserver32[]
                        HKCR\wow6432node\clsid\{25336920-03f9-11cf-8fd0-
 Oueries value:
00aa00686f13}\inprocserver32[threadingmodel]
                        HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_legacy_dispparams[1af5338669efabe0a9841478396871b1.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[1af5338669efabe0a9841478396871b1.exe]
                        HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature object caching[*]
 Queries value:
                        HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
 Queries value:
                        HKLM\system\currentcontrolset\control\wmi\security[9e3b3947-ca5d-4614-
91a2-7b624e0e72441
 Queries value:
                        HKLM\software\wow6432node\microsoft\internet explorer\application
compatibility[1af5338669efabe0a9841478396871b1.exe]
                        HKCU\software\microsoft\internet explorer\domstorage[totallimit]
 Oueries value:
 Oueries value:
                        HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
                        HKCU\software\microsoft\windows
 Queries value:
nt\currentversion\windows[dragscrollinset]
 Oueries value:
                        HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrolldelay]
                        HKCU\software\microsoft\windows
 Oueries value:
nt\currentversion\windows[dragscrollinterval]
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[1af5338669efabe0a9841478396871b1.exe]
 Queries value:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[*]
 Oueries value:
                        HKCR\protocols\handler\about[clsid]
                        HKCR \\ wow 6432 \\ node \\ clsid \\ \{3050f406-98b5-11cf-bb82-00aa00bdce0b\}[]
 Queries value:
                        HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
 Oueries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
 Queries value:
                        HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[]
 Oueries value:
                        HKCR\wow6432node\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
                        HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_protocol_lockdown[1af5338669efabe0a9841478396871b1.exe]
 Oueries value:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
 Oueries value:
                        HKCU\software\microsoft\windows\currentversion\internet
```

settings\zones\3[2106]

```
Oueries value:
                         HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\url history[daystokeep]
                         HKLM\software\policies\microsoft\internet explorer[smartdithering]
 Queries value:
 Oueries value:
                         HKCU\software\microsoft\internet explorer[smartdithering]
 Queries value:
                         HKCU\software\microsoft\internet explorer[rtfconverterflags]
                         HKCU\software\microsoft\internet explorer\main[usecleartype]
 Oueries value:
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[page_transitions]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
                         HKCU\software\microsoft\internet explorer\main[anchor underline]
 Oueries value:
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[css_compat]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[expand alt text]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[display inline images]
                         HKCU\software\microsoft\internet explorer\main[display inline videos]
 Oueries value:
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet explorer\main[display
inline videos]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[play_background_sounds]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[play_animations]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[print_background]
                         HKCU \ \ software \ \ microsoft \ \ internet\ explorer \ \ \ main [use\ stylesheets]
 Oueries value:
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[smoothscroll]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[xmlhttp]
                         HKCU\software\microsoft\internet explorer\main[show image placeholders]
 Oueries value:
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[disable script debugger]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[move system caret]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[force offscreen
composition]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[usethemes]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[usehr]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[q300829]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[cleanup htcs]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[xdomainrequest]
                         HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main[xdomainrequest]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[domstorage]
 Oueries value:
                         HKCU\software\microsoft\internet
explorer\international[default_codepage]
 Queries value:
                         HKCU\software\microsoft\internet explorer\international[autodetect]
 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:
                         HKCU\software\microsoft\internet explorer\settings[anchor color hover]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\settings[always use my colors]
 Queries value:
 Queries value:
                         HKCU\software\microsoft\internet explorer\settings[always use my font
size1
 Oueries value:
                         HKCU\software\microsoft\internet explorer\settings[always use my font
face1
                         HKCU\software\microsoft\internet explorer\settings[disable visited
 Oueries value:
hyperlinks]
 Queries value:
                         HKCU\software\microsoft\internet explorer\settings[use anchor hover
color]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\settings[miscflags]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\policies[allow
programmatic cut_copy_paste]
 Oueries value:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[disablecachingofsslpages]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\pagesetup[print_background]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\codepage[950]
 Queries value:
                         HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsize]
                         HKCU\software\microsoft\internet
 Oueries value:
explorer\international\scripts\3[iefontsizeprivate]
 Queries value:
                         HKCU\software\microsoft\internet
explorer\international\scripts\3[iepropfontname]
                         HKCU\software\microsoft\internet
 Oueries value:
explorer\international\scripts\3[iefixedfontname]
                         HKLM\software\wow6432node\microsoft\internet explorer\version
 Oueries value:
vector[vml]
                         Queries value:
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet explorer\version
vector[windowsedition]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[1af5338669efabe0a9841478396871b1.exe]
                         HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_zone_elevation[*]
 Queries value:
                         HKLM\software\wow6432node\microsoft\internet
```

explorer\main\featurecontrol\feature\_xssfilter[\*] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones[securitysafe] Queries value: HKCU\software\microsoft\internet explorer\main[noprotectedmodebanner] HKLM\software\wow6432node\microsoft\internet explorer\low Oueries value: rights[protectedmodeoffforallzones] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[icon] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zones\0[minlevel] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\zones\0[recommendedlevel] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\0[currentlevel] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1[icon] HKI M\software\wow6432node\microsoft\windows\currentyersion\internet Oueries value: settings\zones\1[minlevel] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings\zones\1[recommendedlevel] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\1[currentlevel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\1[2500] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings\zones\1[2500] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\2[icon] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\zones\2[minlevel] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: 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] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\zones\2[2500] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\3[icon]  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet$ Queries value: settings\zones\3[minlevel] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings\zones\3[recommendedlevel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\3[currentlevel] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[2500] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: 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 Oueries value: settings\zones\4[recommendedlevel] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[currentlevel] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4[2500] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Queries value: settings\zones\4[2500] HKLM\software\wow6432node\microsoft\internet Queries value: explorer\main\featurecontrol\feature\_mshtml\_autoload\_ieframe[1af5338669efabe0a9841478396871b1.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_mshtml\_autoload\_ieframe[\*] HKLM\software\policies\microsoft\windows\currentversion\internet Queries value: settings[cointernetcombineiuricachesize] Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize] HKLM\software\wow6432node\microsoft\windows\currentversion\internet Oueries value: settings[cointernetcombineiuricachesize] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature subdownload lockdown[1af5338669efabe0a9841478396871b1.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_subdownload\_lockdown[\*]  $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ Oueries value: settings[securityidiuricachesize] Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet settings[securitvidiuricachesize] Queries value: HKCU\software\microsoft\windows\currentversion\internet

```
settings[securityidiuricachesize]
   Oueries value:
                                                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[securityidiuricachesize]
    Queries value:
                                                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature sslux[1af5338669efabe0a9841478396871b1.exe]
    Queries value:
                                                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_sslux[*]
                                                         HKLM\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[warnonintranet]
    Queries value:
                                                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings[warnonintranet]
    Queries value:
                                                         \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
settings[warnonintranet]
                                                         HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[]
    Oueries value:
    Queries value:
                                                         HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                                                        HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
    Queries value:
f4ceaaf59cfc}\inprocserver32[]
    Queries value:
                                                        HKCR\wow6432node\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[threadingmodel]
    Queries value:
                                                         HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\progid[]
                                                         HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[]
    Queries value:
                                                        HKCR\wow6432node\clsid\f414c260-6ac0-11cf-b6d1-
    Queries value:
00aa00bbbb58}\inprocserver32[inprocserver32]
   Queries value:
                                                        HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[]
    Queries value:
                                                         HKCR\wow6432node\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
                                                         {\it HKLM \ } \\ {\it software \ } \\ {\it microsoft \ } \\ {\it ole \ } \\ {\it app compat [raise default authnlevel]}
    Oueries value:
    Queries value:
                                                         HKLM\software\microsoft\ole[defaultaccesspermission]
    Queries value:
                                                         HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
    Queries value:
provider[type]
    Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ strong \ cryptographic \ defaults \ provider \ microsoft \ defaults \ provider \
provider[image path]
                                                         HKLM\system\currentcontrolset\control\session
    Oueries value:
manager[safeprocesssearchmode]
                                                         HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
    Queries value:
                                                         HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
    Oueries value:
                                                         HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
    Queries value:
    Oueries 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:
000000000046}\proxystubclsid32[]
                                                        HKLM\software\microsoft\rpc\extensions[remoterpcdll]
    Oueries value:
    Queries value:
                                                         HKCU\software\microsoft\internet explorer\recovery[autorecover]
                                                         HKLM\software\wow6432node\microsoft\internet
    Oueries value:
explorer\main\featurecontrol\feature block lmz img[1af5338669efabe0a9841478396871b1.exe]
    Queries value:
                                                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img[*]
                                                        HKLM\software\wow6432node\microsoft\internet
    Oueries value:
explorer\main\featurecontrol\feature_behaviors[1af5338669efabe0a9841478396871b1.exe]
                                                        HKLM\software\wow6432node\microsoft\internet
    Oueries value:
explorer\main\featurecontrol\feature_behaviors[*]
    Oueries value:
                                                         HKLM\software\wow6432node\microsoft\internet explorer\default
behaviors[homepage]
    Queries value:
                                                         HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\progid[]
                                                         HKCR \land wow6432 node \land [3050f4cf-98b5-11cf-bb82-00aa00bdce0b][]
    Oueries value:
                                                         HKCR \land wow 6432 node \land clsid \land \{3050f4cf-98b5-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb8
    Queries value:
00aa00bdce0b}\inprocserver32[inprocserver32]
                                                         HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
    Oueries value:
00aa00bdce0b}\inprocserver32[]
    Queries value:
                                                        HKCR\wow6432node\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
    Queries value:
                                                        HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\progid[]
                                                         HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[]
    Oueries value:
    Queries value:
                                                        HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32[inprocserver32]
    Oueries value:
                                                        HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32[]
    Queries value:
                                                        HKCR\wow6432node\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32[threadingmodel]
                                                         HKCR \setminus \{d1fe6762 - fc48 - 11d0 - 883a - 3c8b00c10000\}[]
    Queries value:
                                                         HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
    Oueries value:
3c8b00c10000}\inprocserver32[inprocserver32]
                                                        HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
    Oueries value:
3c8b00c10000}\inprocserver32[]
                                                         HKCR\wow6432node\clsid\{d1fe6762-fc48-11d0-883a-
    Oueries value:
3c8b00c10000}\inprocserver32[threadingmodel]
```

Oueries value: HKLM\software\wow6432node\microsoft\internet explorer\default behaviors[dxtfilterbehavior] Oueries value: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[] Queries value: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[inprocserver32] Queries value: HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[] HKCR\wow6432node\clsid\{4fd2a832-86c8-11d0-8fca-Oueries value: 00c04fd9189d}\inprocserver32[threadingmodel] Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath] Oueries value: Queries value: HKLM\hardware\devicemap\video[maxobjectnumber] Queries value: HKLM\hardware\devicemap\video[\device\video3] HKLM\system\currentcontrolset\control\video\{43056cc8-3bf6-4ce7-bd67-Oueries value: 1e1a187c13e9}\0000[pruningmode] HKLM\hardware\devicemap\video[\device\video0] Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-Oueries value: 9dd4432fa2e9}\0000[pruningmode] HKLM\hardware\devicemap\video[\device\video1] Queries value: Oueries value: 0d8e74595f78}\0000[pruningmode] HKLM\hardware\devicemap\video[\device\video2] Queries value: Oueries value: 8ed0c8eb59a8}\0000[pruningmode] HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![name] Queries value: Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![flags] HKLM\software\wow6432node\microsoft\directdraw\compatibility\bug![id] Queries value: Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2[name] HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2[flags] Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\demolitionderby2[id] Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibilitv\diablo[flags] Oueries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\diablo[id] Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[name] Oueries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[flags] Oueries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\mortalkombat3[id] Oueries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[name] Queries value:  $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus direct draw \setminus compatibility \setminus msgolf 98[flags]$ Oueries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\msgolf98[id] Oueries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[name] Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[flags] Oueries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nhlpowerplay[id] Oueries value:  $HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus direct draw \setminus compatibility \setminus norton system in fo[name]$ Oueries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[flags] Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\nortonsysteminfo[id] Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue squadron[name] Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue squadron[flags] HKLM\software\wow6432node\microsoft\directdraw\compatibility\rogue Queries value: squadron[id] Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibilitv\savage[name] Queries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[flags] HKLM\software\wow6432node\microsoft\directdraw\compatibility\savage[id] Oueries value: Queries value:  $HKLM \ software \ wow 6432 node \ microsoft \ direct draw \ compatibility \ scorched planet [name]$ Oueries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[flags] Oueries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\scorchedplanet[id] Oueries value: HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[name]

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| directdraw\\| compatibility\\| silentthunder[flags]|$ 

Oueries value:

```
Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\silentthunder[id]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[name]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[flags]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft100[id]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[name]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraft115[flags]
  Oueries value:
Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[name]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[flags]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\starcraftdemo[id]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide[name]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide[flags]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\terracide[id]
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[name]
  Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[flags]
  Queries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\thirddimension[id]
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
  Oueries value:
Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus direct draw \setminus compatibility \setminus ziff daviswinmark benchmark [name]
  Oueries value:
Oueries value:
HKLM\software\wow6432node\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
                                    HKLM\software\wow6432node\microsoft\directdraw[modexonly]
  Oueries value:
                                    HKLM\software\wow6432node\microsoft\directdraw[emulationonly]
  Queries value:
  Oueries value:
                                    HKLM\software\wow6432node\microsoft\directdraw[showframerate]
  Queries value:
                                    HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus direct draw[enable printscreen] \\
  Oueries value:
                                    HKLM\software\wow6432node\microsoft\directdraw[forceagpsupport]
  Oueries value:
                                    HKLM\software\wow6432node\microsoft\directdraw[disableagpsupport]
                                    HKLM\software\wow6432node\microsoft\directdraw[disablemmx]
  Oueries value:
  Oueries value:
                                    HKLM\software\wow6432node\microsoft\directdraw[disableddscapsinddsd]
  Oueries value:
                                    HKLM\software\wow6432node\microsoft\directdraw[disablewidersurfaces]
  Queries value:
                                    HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus direct draw[use nonlocal vid mem] \\
                                    HKLM\software\wow6432node\microsoft\directdraw[forcerefreshrate]
  Oueries value:
  Queries value:
                                    HKLM\software\wow6432node\microsoft\direct3d[flipnovsync]
  Oueries value:
                                    HKLM\software\wow6432node\microsoft\directdraw[owndc]
                                    HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\progid[]
  Oueries value:
  Oueries value:
                                    HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[]
                                    HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
  Queries value:
f941e9b7e1fe}\inprocserver32[inprocserver32]
  Oueries value:
                                   HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[]
                                    HKCR\wow6432node\clsid\{a7ee7f34-3bd1-427f-9231-
  Oueries value:
f941e9b7e1fe}\inprocserver32[threadingmodel]
                                    HKCR\dximagetransform.microsoft.shadow\clsid[]
  Oueries value:
  Queries value:
                                    HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}\progid[]
  Oueries value:
                                    HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-00c04fa34f05}[]
  Queries value:
                                    HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
00c04fa34f05}\inprocserver32[]
                                   HKCR\wow6432node\clsid\{e71b4063-3e59-11d2-952a-
  Oueries value:
00c04fa34f05}\inprocserver32[threadingmodel]
  Queries value:
                                    HKCR \setminus \{4cb26c03 - ff93 - 11d0 - 817e - 0000f87557db\}[]
  Oueries value:
                                    HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[inprocserver32]
                                    HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-817e-12d0-8
  Oueries value:
0000f87557db}\inprocserver32[1
  Oueries value:
                                    HKCR\wow6432node\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[threadingmodel]
                                    HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\progid[]
```

 $HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd\}[]$ 

Queries value: Queries value:

```
Queries value:
                                     HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[inprocserver32]
                                     HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Oueries value:
f4fc1e6ca1bd}\inprocserver32[]
                                     HKCR\wow6432node\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Oueries value:
f4fc1e6ca1bd}\inprocserver32[threadingmodel]
                                     \label{limits} \begin{tabular}{ll} HKCR \typelib \end{tabular} -37c-11d1-b047-00aa003b6061 \end{tabular} \label{limits} 1.1\0\win32[]
  Oueries value:
                                     HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]
  Oueries value:
  Oueries value:
                                     HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-00aa003f8646}[]
  Oueries value:
                                     HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
00aa003f8646}\inprocserver32[]
                                     HKCR\wow6432node\clsid\{275c23e2-3747-11d0-9fea-
  Oueries value:
00aa003f8646}\inprocserver32[threadingmodel]
                                     HKLM\system\currentcontrolset\control\nls\codepage[1250]
  Queries value:
  Queries value:
                                     HKLM\svstem\currentcontrolset\control\nls\codepage[1251]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1253]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1254]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1255]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1256]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1257]
  Queries value:
                                     HKLM\svstem\currentcontrolset\control\nls\codepage[1258]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[874]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[932]
  Oueries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[936]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[949]
  Queries value:
                                     HKLM\system\currentcontrolset\control\nls\codepage[1361]
                                     HKCU\software\microsoft\internet
  Oueries value:
explorer\international\scripts\26[iefontsize]
                                     HKCU\software\microsoft\internet
  Oueries value:
explorer\international\scripts\26[iefontsizeprivate]
                                     HKCU\software\microsoft\internet
  Queries value:
explorer\international\scripts\26[iepropfontname]
  Oueries value:
                                     HKCU\software\microsoft\internet
explorer\international\scripts\26[iefixedfontname]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane1]
                                     HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane2]
  Oueries value:
                                     HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane3]|
  Oueries value:
                                     HKLM\svstem\currentcontrolset\services\netbt\linkage[export]
  Queries value:
                                     HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane4]|
                                     HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane5]
                                     HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane6]
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane7]
                                     HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane8]
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane9]
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane10]
                                     HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane11]
                                     HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback\simsun[plane12]|
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane13]
                                     HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane14]
                                     HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback\simsun[plane15]
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\simsun[plane16]
                                     HKCU\software\microsoft\windows script\settings[jitdebug]
  Oueries value:
  Queries value:
                                     HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32[]
                                     HKCR\wow6432node\interface\{332c4425-26cb-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-11d0-b483-6cd-
  Oueries value:
00c04fd90119}\proxystubclsid32[]
  Queries value:
                                     \label{locality} \mbox{HKCR} $$ \mbox{Wow} 6432 \mbox{node} \mbox{clsid} \mbox{00020424-0000-0000-c000-00000000046} [\mbox{\sc i}] $$
  Oueries value:
                                     HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32[inprocserver32]
                                     HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
  Oueries value:
00000000046}\inprocserver32[]
                                     Oueries value:
00000000046}\inprocserver32[threadingmodel]
                                     HKCR\mime\database\content type\image/png[extension]
  Oueries value:
  Queries value:
                                     \label{locality} HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\progid[]\\
```

```
HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[]
 Oueries value:
 Oueries value:
                         HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
 Queries value:
00aa006c1a01}\inprocserver32[1
 Queries value:
                         HKCR\wow6432node\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
                         HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\progid[]
 Oueries value:
 Oueries value:
                         HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[]
                          HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
 Queries value:
00aa006c1a01}\inprocserver32[inprocserver32]
 Queries value:
                         HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[]
                         HKCR\wow6432node\clsid\{6a01fda0-30df-11d0-b724-
 Oueries value:
00aa006c1a01}\inprocserver32[threadingmodel]
                         HKCR\mime\database\content type\image/bmp\bits[0]
 Queries value:
                         HKCR\mime\database\content type\image/gif\bits[0]
 Oueries value:
 Queries value:
                          HKCR\mime\database\content type\image/jpeg\bits[0]
 Queries value:
                          HKCR\mime\database\content type\image/pjpeg\bits[0]
 Oueries value:
                          HKCR\mime\database\content type\image/png\bits[0]
 Queries value:
                          HKCR\mime\database\content type\image/x-png\bits[0]
                          HKCR\mime\database\content type\image/x-wmf\bits[0]
 Queries value:
                          HKCR\mime\database\content type\image/x-png[image filter clsid]
 Oueries value:
 Queries value:
                          HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\progid[]
 Queries value:
                          HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[]
                         HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
 Queries value:
00a0c913f750}\inprocserver32[inprocserver32]
 Queries value:
                         HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[]
                         HKCR\wow6432node\clsid\{a3ccedf7-2de2-11d0-86f4-
 Queries value:
00a0c913f750}\inprocserver32[threadingmodel]
                         HKLM\software\wow6432node\microsoft\direct3d[disablemmx]
 Queries value:
                         HKLM\software\wow6432node\microsoft\direct3d[disablex3d]
 Queries value:
 Queries value:
                          HKLM\software\wow6432node\microsoft\direct3d[fewvertices]
                         HKLM\software\wow6432node\microsoft\direct3d[disablevidmemvbs]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_block_lmz_script[1af5338669efabe0a9841478396871b1.exe]
                         HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_block_lmz_script[*]
                         HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
 Queries value:
 Oueries value:
                         HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
 Oueries value:
00c04fb6bfc4}\inprocserver32[]
                         HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
 Oueries value:
00c04fb6bfc4}\inprocserver32[threadingmodel]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2000]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\internet explorer\feed
discovery[sound]
 Queries value:
                          HKCU\software\microsoft\ftp[use web based ftp]
                          HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}[]
 Oueries value:
 Queries value:
                         HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[inprocserver32]
                         HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
 Oueries value:
fd2b31b3eefd}\inprocserver32[]
                         HKCR\wow6432node\clsid\{e569bde7-a8dc-47f3-893f-
 Oueries value:
fd2b31b3eefd}\inprocserver32[threadingmodel]
                         HKCR\mime\database\content type\image/gif[extension]
 Oueries value:
                         HKCU\software\microsoft\internet
 Queries value:
explorer\services[selectionactivitybuttondisable]
                         \label{lem:hkcu} \verb+KKCU\software\microsoft\internet explorer\suggested sites[enabled]
 Oueries value:
                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[attributes]
                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[callforattributes]
 Queries value:
                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[restrictedattributes]
 Queries value:
                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
 Queries value:
                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
 Oueries value:
                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
 Queries value:
                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Queries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 Oueries value:
08002b30309d}\shellfolder[queryforoverlay]
 Queries value:
                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[mapnetdriveverbs]
 Queries value:
                         HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
```

```
08002b30309d}\shellfolder[queryforinfotip]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[hideinwebview]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideondesktopperuser]
  Queries value:
                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsaliasednotifications]
                                    HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsuniversaldelegate]
  Oueries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
  Oueries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hasnavigationenum]
  Oueries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus monenum [\{20d04fe0-3aea-1069-a2d8-microsoft\}] + \{20d04fe0-3aea-1069-a2d8-microsoft\} + \{20d04fe0-3aea-1060-a2d8-microsoft\} + \{20d04fe0-3aea-1060-a2d8-mi
08002b30309d}]
  Queries value:
11e3-a68e-806e6f6e6963}[data]
  Queries value:
11e3-a68e-806e6f6e6963}[generation]
                                     HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
  Queries value:
409d6c4515e9}[drivemask]
                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
  Queries value:
                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Queries value:
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                     HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Queries value:
b8dc300d9f9d}\inprocserver32[]
                                    HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Queries value:
b8dc300d9f9d}\inprocserver32[threadingmodel]
  Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]|
                                     HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
  Queries value:
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
  Oueries value:
                                     \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced| fidden] \end{tabular}
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
  Oueries value:
11e3-a68e-806e6f6e6963}[data]
  Queries value:
11e3-a68e-806e6f6e6963}[generation]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
  Queries value:
                                     HKCR\directory[docobject]
  Oueries value:
                                     HKCR\folder[docobject]
  Queries value:
                                     HKCR\allfilesystemobjects[docobject]
```

```
Oueries value:
                          HKCR\directory[browseinplace]
                          HKCR\folder[browseinplace]
 Oueries value:
 Oueries value:
                          HKCR\allfilesystemobjects[browseinplace]
 Queries value:
                          HKCR\directory[isshortcut]
                          HKCR\folder[isshortcut]
 Oueries value:
 Queries value:
                          HKCR\allfilesystemobjects[isshortcut]
 Oueries value:
                          HKCR\directory[alwaysshowext]
                          HKCR\directory[nevershowext]
 Oueries value:
 Queries value:
                          HKCR\folder[nevershowext]
 Queries value:
 Oueries value:
444553540000}\inprocserver32[]
 Queries value:
444553540000}\inprocserver32[loadwithoutcom]
 Queries value:
```

HKCR\allfilesystemobjects[nevershowext]

 $HKCR\wow6432node\clsid\ff393560-c2a7-11cf-bff4-$ 

HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-

HKCU\software\microsoft\windows\currentversion\shell

extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {000214e6-0000-0000-c000-000000000046}}

0xffff1

Queries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[]

Queries value:  $HKCR\wow6432node\clsid\ff393560-c2a7-11cf-bff4-$ 

444553540000}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\inprocserver32[threadingmodel]

HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache\extensible cache\mshist012016042220160423[cacherepair] HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]

HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\extensible cache\mshist012016042220160423[cacheprefix]

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

settings\5.0\cache\extensible cache\mshist012016042220160423[cachelimit] HKCU\software\microsoft\windows\currentversion\internet Oueries value:

settings\5.0\cache\extensible cache\mshist012016042220160423[cacheoptions]  $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-d10d + (20d04fe0-d10d + (20d04fe0-d1$ Queries value:

3aea-1069-a2d8-08002b30309d}[]

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

08002b30309d}[localizedstring]

HKCU\software\microsoft\internet Oueries value:

explorer\main\windowssearch[enabledscopes]

68ad-4d8a-87bd-30b759fa33dd}[category]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[name]

68ad-4d8a-87bd-30b759fa33dd}[parentfolder]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[description] Oueries value:

68ad-4d8a-87bd-30b759fa33dd}[relativepath]

68ad-4d8a-87bd-30b759fa33dd}[parsingname] Oueries value:

68ad-4d8a-87bd-30b759fa33dd}[infotip]

68ad-4d8a-87bd-30b759fa33dd}[localizedname]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[icon]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[security]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1777f761-68ad-4d8a-87bd-30b759fa33dd}[streamresource]

68ad-4d8a-87bd-30b759fa33dd}[streamresourcetype]

Queries value:

68ad-4d8a-87bd-30b759fa33dd}[localredirectonly]

68ad-4d8a-87bd-30b759fa33dd}[roamable]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1777f761-161644, 1777f761-16164, 1777f761-1616$ 68ad-4d8a-87bd-30b759fa33dd}[precreate]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-68ad-4d8a-87bd-30b759fa33dd\} \ folder \ descriptions \ folder \ folder \ descriptions \ folder \ fol$ 

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-68ad-4d8a-87bd-30b759fa33dd\} [publish expanded path]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-68ad-4d8a-87bd-30b759fa33dd\} [attributes]$ 

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1777f761-68ad-4d8a-87bd-30b759fa33dd\} [initfolder handler]$ 

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

folders[favorites]

Queries value: HKLM\software\wow6432node\microsoft\windows search[currentversion]
Queries value: HKLM\software\wow6432node\microsoft\downloadmanager[cacheok]
Queries value: HKCR\mime\database\content type\image/x-icon[extension]

Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasapi32[enablefiletracing] Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasapi32[enableconsoletracing]
Sets/Creates value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 1af5338669 efabe 0a9841478396871b1\_rasapi32 [file tracing mask] \\ Sets/Creates \ value:$ 

HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasapi32[consoletracingmask] Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasapi32[maxfilesize]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasapi32[filedirectory]

HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasmancs[enablefiletracing]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasmancs[enableconsoletracing]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasmancs[filetracingmask] Sets/Creates value:

 $HKLM \ software \ wow 6432 node \ microsoft \ tracing \ 1af5338669 efabe 0a9841478396871b1\_rasmancs \ [consoletracing mask] \\ Sets \ / Creates \ value:$ 

HKLM\software\wow6432node\microsoft\tracing\1af5338669efabe0a9841478396871b1\_rasmancs[maxfilesize]
Sets/Creates value:

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012016042220160423[cacheprefix]

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012016042220160423[cachelimit]

 $Sets/Creates\ value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible\ cache\mbox{\sc missol2016042220160423} [cacheoptions]$ 

settings\5.0\cache\extensible cache\mshist012016042220160423[cacherepair]

Value changes: HKCU\software\microsoft\internet explorer\main[disable script debugger]

HKCU\software\microsoft\windows\currentversion\internet

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

settings\zonemap[uncasintranet]

 $\label{thm:condition} Value\ changes: \\ HKCU \ software \ microsoft \ windows \ current version \ internet$ 

settings\zonemap[autodetect]

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

settings[proxyenable]

Sets/Creates value:

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

settings\connections[savedlegacysettings]

Value changes:

 $HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| direct draw \verb|\mostrecentapplication[name]|$ 

Value changes: HKLM\software\wow6432node\microsoft\directdraw\mostrecentapplication[id] Value changes: HKLM\software\wow6432node\microsoft\direct3d\mostrecentapplication[name]

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

settings\5.0\cache\extensible cache\mshist012016042220160423[cachepath]

Value changes: HKCU\software\microsoft\internet explorer\main\windowssearch[version]