Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3310, Task ID: 748

Task ID: 748 Risk Level: 10

Date Processed: 2016-05-18 10:33:24 (UTC)

Processing Time: 17.21 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6b1383f452de6d7b6d9a656c24904858.exe"

Sample ID: Type: basic admin Owner:

6b1383f452de6d7b6d9a656c24904858 Label:

Date Added: 2016-05-18 10:30:49 (UTC) PE32:win32:gui

File Type: File Size: 86016 bytes

6b1383f452de6d7b6d9a656c24904858 MD5:

6bfd319db22de02b3658e3618808b2e72ac4ddc8937ac2fd046a6b7e87b768a7 SHA256:

Description: None

Pattern Matching Results

3 Long sleep detected

4 Terminates process under Windows subfolder

10 Creates malicious events: Beebone [Trojan]

6 Checks task list from command line

Process/Thread Events

C:\WINDOWS\Temp\6b1383f452de6d7b6d9a656c24904858.exe Creates process:

["c:\windows\temp\6b1383f452de6d7b6d9a656c24904858.exe"]

C:\WINDOWS\system32\cmd.exe ["C:\WINDOWS\system32\cmd.exe" /c Creates process:

tasklist&&del 6b1383f452de6d7b6d9a656c24904858.exe]

C:\WINDOWS\system32\tasklist.exe [tasklist] Creates process:

Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs] Terminates process: C:\WINDOWS\Temp\6b1383f452de6d7b6d9a656c24904858.exe

Terminates process: C:\WINDOWS\system32\tasklist.exe Terminates process: C:\WINDOWS\system32\cmd.exe

Named Object Events

Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003 Creates mutex:

\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex:

\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex:

\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex:

\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates mutex:

\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003 \BaseNamedObjects\c:!documents and settings!admin!local Creates mutex:

settings!temporary internet files!content.ie5!

Creates mutex: \BaseNamedObjects\c:!documents and settings!admin!cookies! \BaseNamedObjects\c:!documents and settings!admin!local Creates mutex:

settings!history!history.ie5!

\BaseNamedObjects\WininetConnectionMutex Creates mutex: \BaseNamedObjects\ZonesCounterMutex Creates mutex:

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

Creates mutex: \BaseNamedObjects\SHIMLIB_LOG_MUTEX

\BaseNamedObjects\userenv: User Profile setup event Creates event:

\BaseNamedObjects\C:?WINDOWS?TEMP?6B1383F452DE6D7B6D9A656C24904858.EXE Creates semaphore: Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57} Creates semaphore:

File System Events

Opens: C:\WINDOWS\Prefetch\6B1383F452DE6D7B6D9A656C24904-1F30805C.pf

Opens: C:\Documents and Settings\Admin Opens: C:\WINDOWS\system32\msvbvm60.dll Opens: C:\WINDOWS\system32\imm32.dll Opens: C:\WINDOWS\system32\rpcss.dll C:\WINDOWS\system32\MSCTF.dll Opens: Opens: C:\WINDOWS\system32\sxs.dll ${\tt C:\WINDOWS\system32\MSCTFIME.IME}$ Opens: Opens: C:\WINDOWS\system32\winmm.dll

```
C:\WINDOWS\Temp\6b1383f452de6d7b6d9a656c24904858.exe
 Opens:
 Opens:
                         C:\
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
 Opens:
                         C:\WINDOWS\WindowsShell.Manifest
                         C:\WINDOWS\WindowsShell.Config
 Opens:
 Opens:
                         C:\WINDOWS\system32\wininet.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\wininet.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Cookies
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\index.dat
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rasman.dll
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
 Opens:
                         C:\AUTOEXEC.BAT
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
                         C:\WINDOWS\system32\ras
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
                         C:\WINDOWS\system32\sensapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS\system32\msv1_0.dll
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
                         C:\WINDOWS\system32\ieframe.dll.123.Config
 Opens:
 Opens:
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\WINDOWS
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
                         C:\WINDOWS\system32\cmd.exe
                         {\tt C:\WINDOWS\AppPatch\symmin.sdb}
 Opens:
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
                         C:\WINDOWS\system32\cmd.exe.Manifest
                         C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
 Opens:
 Opens:
                         C:\WINDOWS\WINHELP.INI
 Opens:
                         C:
                         C:\WINDOWS\AppPatch
 Opens:
 Opens:
                         C:\WINDOWS\system32\wbem
 Opens:
                         C:\WINDOWS\WinSxS
                         C:\WINDOWS\system32\ntdll.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\kernel32.dll
 Opens:
                         C:\WINDOWS\system32\unicode.nls
 Opens:
                         C:\WINDOWS\system32\locale.nls
 Opens:
                         C:\WINDOWS\system32\sorttbls.nls
 Opens:
                         C:\WINDOWS\svstem32\msvcrt.dll
 Opens:
                         C:\WINDOWS\system32\user32.dll
```

C:\WINDOWS\system32\gdi32.dll Opens: Opens: C:\WINDOWS\system32\shimeng.dll C:\WINDOWS\AppPatch\AcGenral.dll Opens: Opens: C:\WINDOWS\system32\advapi32.dll Opens: C:\WINDOWS\system32\rpcrt4.dll Opens: C:\WINDOWS\system32\secur32.dll C:\WINDOWS\system32\ole32.dll Opens: Opens: C:\WINDOWS\system32\oleaut32.dll Opens: C:\WINDOWS\system32\msacm32.dll Opens: C:\WINDOWS\system32\version.dll Opens: C:\WINDOWS\svstem32\shlwapi.dll Opens: C:\WINDOWS\system32\userenv.dll Opens: C:\WINDOWS\system32\uxtheme.dll Opens: C:\WINDOWS\system32\ctype.nls Opens: C:\WINDOWS\system32\sortkey.nls Opens: C:\WINDOWS\system32\apphelp.dll Opens: C:\WINDOWS\system32\wbem\wmic.exe Opens: C:\Documents and Settings

Opens: C:\WINDOWS\system32\tasklist.exe
Opens: C:\WINDOWS\system32\tasklist.exe.Manifest

Opens: C:\WINDOWS\Prefetch\TASKLIST.EXE-10D94B23.pf Opens: C:\WINDOWS\system32\wbem\framedyn.dll Opens: C:\WINDOWS\system32\dbghelp.dll Opens: C:\WINDOWS\system32\winlogon.exe Opens: C:\WINDOWS\system32\xpsp2res.dll C:\WINDOWS\system32\wbem\wbemprox.dll Opens: Opens: C:\WINDOWS\system32\wbem\wbemcomn.dll Opens: C:\WINDOWS\system32\winsta.dll C:\WINDOWS\system32\wbem\wbemsvc.dll

Opens: C:\WINDOWS\system32\wbem\wbemsvc.dll
Opens: C:\WINDOWS\system32\wbem\fastprox.dll
Opens: C:\WINDOWS\system32\msvcp60.dll
Opens: C:\WINDOWS\system32\ntdsapi.dll

 $\label{lem:c:windows} Reads from: C: \windows \temp\6b1383f452de6d7b6d9a656c24904858.exe$

Reads from: C:\AUT0EXEC.BAT

Reads from: C:\WINDOWS\system32\drivers\etc\hosts
Reads from: C:\WINDOWS\system32\rsaenh.dll

 $\label{lem:c:windows} $$ Reads from: $$ C:\WINDOWS\Registration\R00000000007.clb $$$

Reads from: C:\WINDOWS\system32\cmd.exe

Reads from: C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf

Network Events

DNS query: domai.1noip.org
Sends data to: 8.8.8.8:53
Receives data from: 0.0.0.0:0

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders

Creates key: HKLM\software\microsoft\tracing

Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders

Creates key: HKCU\software\microsoft\windows nt\currentversion\winlogon

Creates key: HKLM\software\microsoft\windows\currentversion\explorer\shell folders

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

 ${\tt settings \backslash connections}$

 $\label{lem:creates} \begin{tabular}{lll} \label{lem:creates} $$\operatorname{HKCU}\operatorname{software}\operatorname{microsoft}\operatorname{windows} \ \operatorname{nt}\operatorname{currentversion}\operatorname{network}\operatorname{location} $$$

awareness

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

Creates key:

HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\0000000000008352

Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\blocked
Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
Creates key: HKLM\software\microsoft\windows\currentversion\shell extensions\cached
Creates key: HKCU\software\microsoft\windows\currentversion\shell extensions\cached
Creates key: Creates key:

 $\label{lem:hkcu} HKCU software \microsoft \windows \current version \explorer \mountpoints 2 \f 90255c2-6bc4-11e3-9fc7-806d6172696f \end{picture}$

Creates key: HKCU\software\microsoft\visual basic\6.0

Creates key: HKCU\software

Creates key: HKCU\software\microsoft

Creates key: HKCU\software\microsoft\visual basic Creates key: HKCU\software\microsoft\multimedia\audio

Creates key: HKCU\software\microsoft\multimedia\audio compression manager\
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\msacm
Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority

v4.00

Creates key: HKLM\software\microsoft\wbem\cimom

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\6b1383f452de6d7b6d9a656c24904858.exe

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

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

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

options\gdi32.dll

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

options\user32.dll

Opens key: HKLM\system\currentcontrol\session manager

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

options\imm32.dll

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

options\ntdll.dll

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

options\kernel32.dll

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

options\secur32.dll

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

options\rpcrt4.dll

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

options\advapi32.dll

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

options\msvcrt.dll

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

options\ole32.dll

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

options\oleaut32.dll

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

options\msvbvm60.dll

Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

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

Opens key: HKLM\

Opens key: ${\tt HKLM\backslash software\backslash microsoft\backslash windows\ nt\backslash current version\backslash diagnostics}$

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

Opens key: HKCR\interface\{00020400-0000-0000-0000-000000000046}

Opens key: HKLM\software\microsoft\oleaut

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

Opens key: HKCU\

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

Opens kev: HKCU\control panel\desktop

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

options\msctf.dll

Opens key:

Opens key: HKLM\software\microsoft\ctf\systemshared\

Opens key: HKCU\keyboard layout\toggle
Opens key: HKLM\software\microsoft\ctf\

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

options\sxs.dll

Opens key: HKLM\system\setup

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

Opens key: ${\tt HKLM \backslash software \backslash microsoft \backslash windows\ nt \backslash current version \backslash image\ file\ execution}$

options\version.dll

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

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

Opens key: ${\tt HKLM \backslash software \backslash microsoft \backslash ctf \backslash systems hared}$

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

Opens key: HKLM\software\microsoft\vba\monitors

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

options\winmm.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32

Opens kev:

Opens key: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm

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

Opens key: HKLM\software\microsoft\rpc

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

options\6b1383f452de6d7b6d9a656c24904858.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKCU\software\microsoft\multimedia\sound mapper

Opens key: HKCU\software\microsoft\windows\currentversion\multimedia\midimap

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

panel\international\calendars\twodigityearmax

Opens key: HKCU\control panel\international\calendars\twodigityearmax

Opens key: HKLM\system\currentcontrolset\services\disk\enum

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

options\shlwapi.dll

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

options\normaliz.dll

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

options\iertutil.dll

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

options\urlmon.dll

Opens key:

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

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

options\comctl32.dll

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\lz32.dll

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

options\wininet.dll

Opens key: HKCU\software\classes\

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

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

settings

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

settings

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

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

settings\

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

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915

Opens key: HKLM\software\microsoft\internet

 $\label{lem:control} explorer $$ explorer \rightarrow \frac{1}{esc_{enabled_kb918915}} $$ Opens key: $$ HKLM \circ \frac{1}{esc_{enabled_kb918915}} $$ explorer \rightarrow \frac{1}{esc_{enabled_kb918915}} $$ Opens key: $$ HKLM \circ \frac{1}{esc_{enabled_kb918915}} $$ explorer \rightarrow \frac{1}{esc_{enabled_kb918915}} $$ Opens key: $$ HKLM \circ \frac{1}{esc_{enabled_kb918915}} $$ explorer \rightarrow \frac{1}{esc_{enabled_kb918915}} $$ expl$

settings\zonemap\domains\
Opens key:

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

settings\zonemap\domains\

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

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\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck

Opens key: HKLM\system\currentcontrolset\control\wmi\security

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

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

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

settings\5.0\cache

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

settings\5.0\cache

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

settings\5.0\cache\content

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

settings\5.0\cache\content

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

options\shell32.dll

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

settings\5.0\cache\cookies

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

settings\5.0\cache\cookies

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

settings\5.0\cache\history

```
Opens key:
                         HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
 Opens key:
                         HKLM\system\currentcontrolset\control\computername
                         HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens key:
 Opens kev:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
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\mshist012014033120140407
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\mshist012014041220140413
 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\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache
                         HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                         HKLM\software\microsoft\internet
 Opens key:
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
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                         HKLM\software\microsoft\internet
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\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\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\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
 Opens key:
                         HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
```

Opens kev:

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001 Opens kev:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens kev:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011 Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004 Opens kev:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_http_username_password_disable

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\netapi32.dll

Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasman.dll

Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\rtutils.dll

Opens key:

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

options\tapi32.dll

Opens key: HKLM\software\microsoft\windows\currentversion\telephony

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

options\rasapi32.dll

Opens key: HKLM\software\microsoft\tracing\rasapi32

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

options\userenv.dll

Opens key: HKLM\system\currentcontrolset\control\productoptions

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

folders

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

Opens kev: HKLM\software\microsoft\windows nt\currentversion\profilelist Opens key: HKLM\system\currentcontrolset\control\session manager\environment

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

Opens key: HKU\

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

1757981266-507921405-1957994488-1003 HKCU\environment Opens kev:

Opens key: HKCU\volatile environment

 $\label{lem:hklmsoftware} \mbox{\tt HKLM\software\mbox{\tt microsoft\windows}\ nt\current version\space{\tt version}} \mbox{\tt image file execution}$ Opens key:

options\sensapi.dll

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

filters\rpa Opens kev: HKLM\software\microsoft\windows\currentversion\internet settings\http

filters\rpa

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209 Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling

```
Opens key:
                                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options\rasadhlp.dll
   Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
   Opens key:
                                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                                                  HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
   Opens key:
                                                  \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings\zonemap\protocoldefaults\
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\domains\
  Opens key:
                                                  HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
   Opens key:
                                                  HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com
                                                  HKLM\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\domains\msn.com\related
                                                  HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
                                                  HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
   Opens key:
                                                  HKCU\software\microsoft\internet explorer\ietld
   Opens key:
                                                  HKLM\software\policies\microsoft\internet explorer\security
   Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\internet settings\zones\
                                                  \label{lem:hkcu} \mbox{\current} windows \mbox{\current} internet settings \mbox{\current} settings \mbox{\current} and \mbo
   Opens key:
   Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
   Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
                                                  \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\zones\3}}
   Opens key:
   Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
   Opens key:
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\
   Opens key:
                                                  HKLM \verb|\software\policies\microsoft\windows\currentversion\ | internet
settings\zones\0
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zones\0
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\1
   Opens key:
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zones\2
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\2
   Opens key:
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\3
   Opens key:
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\4
                                                  HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
                                                  HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
   Opens key:
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                                  \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
  Opens key:
settings\lockdown_zones\
   Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
   Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\0
  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\lockdown_zones\0
   Opens key:
                                                  \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\lockdown_zones\1
                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\1
   Opens key:
                                                  \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\lockdown_zones\1
```

HKCU\software\microsoft\windows\currentversion\internet

Opens key:

```
settings\lockdown_zones\2
                                                                    HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens kev:
 settings\lockdown_zones\2
                                                                     \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
     Opens key:
settings\lockdown_zones\2
                                                                     \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
    Opens key:
 settings\lockdown_zones\3
    Opens key:
                                                                    HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\lockdown_zones\3
     Opens key:
                                                                    HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
     Opens key:
                                                                     HKCU\software\microsoft\windows\currentversion\internet
 settings\lockdown_zones\4
                                                                    HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens key:
 settings\lockdown_zones\4
     Opens key:
                                                                    HKCU\software\policies\microsoft\windows\currentversion\internet
 settings\lockdown_zones\4
     Opens key:
                                                                    HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                                                    HKLM\software\microsoft\internet
    Opens key:
 explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
     Opens key:
                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
     Opens key:
                                                                     HKLM\system\currentcontrolset\services\dnscache\parameters
     Opens key:
                                                                     HKLM\software\policies\microsoft\windows nt\dnsclient
     Opens key:
                                                                     HKLM\system\currentcontrolset\services\tcpip\parameters
     Opens key:
                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\iphlpapi.dll
                                                                     HKLM\system\currentcontrolset\services\tcpip\linkage
     Opens kev:
     Opens key:
                                                                     HKLM\system\currentcontrolset\services\tcpip\parameters\
     Opens key:
                                                                     HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
     Opens key:
                                                                     {\tt HKLM \ } system \verb|\currentcontrolset \ } net bt \verb|\parameters|
     Opens key:
c7d49d7cecdc}
     Opens key:
                                                                     HKLM\software\policies\microsoft\system\dnsclient
     Opens key:
                                                                     HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
 cryptographic provider
     Opens key:
                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
                                                                     HKLM\software\microsoft\rpc\securityservice
     Opens key:
     Opens key:
                                                                     HKLM\software\policies\microsoft\cryptography
     Opens key:
                                                                     HKLM\software\microsoft\cryptography
                                                                     {\tt HKLM \coftware \microsoft \cryptography \coffload}
     Opens key:
     Opens key:
                                                                     HKLM\system\currentcontrolset\control\securityproviders
     Opens key:
                                                                     HKLM\system\currentcontrolset\control\lsa\sspicache
                                                                     HKLM \ system \ current control \ lsa \ sspicache \ msaps spc. dll
     Opens key:
     Opens key:
                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens kev:
 options\hnetcfg.dll
     Opens key:
                                                                     HKLM\system\currentcontrolset\services\winsock\parameters
     Opens key:
                                                                     HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
     Opens key:
                                                                     HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
     Opens key:
                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
                                                                     {\tt HKLM \ } system \verb|\ current control \ } security providers \verb|\ sasl profiles \ |
     Opens key:
     Opens key:
                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msv1_0.dll
                                                                     HKLM\system\currentcontrolset\services\netbt\linkage
     Opens key:
     Opens key:
Opens key:
                                                                    HKCU\software\microsoft\windows\currentversion\explorer
     Opens key:
                                                                     HKLM\software\microsoft\windows\currentversion\explorer
     Opens key:
                                                                     HKLM\software\microsoft\windows\currentversion\policies\explorer
     Opens key:
                                                                    HKCU\software\microsoft\windows\currentversion\policies\explorer
     Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace
     Opens key:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{11016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d22-d1016101-e366-4d20-d1016101-e366-4d20-d1016101-e366-4d20-d1016101-e366-4d20-d1016101-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d101610-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d10160-e366-4d20-d100-e366-4d20-d100-e366-4d20-d100-e366-4d20-d100-e366-4d0-e366-4d0-e366-4d0-e366-4d00
bc06-4ada335c892b}
     Opens key:
ba4f-00a0c91eedba}
     Opens key:
HKLM \ software \ microsoft \ windows \ current version \ explorer \ desktop \ namespace \ \{450d8fba-ad25-11d0-desktop \ namespace \ for the sum of the 
98a8-0800361b1103}
     Opens key:
9f08-00aa002f954e}
     Opens key:
HKLM \label{lem:hklm} Which is the statement of the sta
83f2-00a0c90dc849}
     Opens key:
```

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

Opens key:

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

08002b30309d}\shellfolder

 $HKCR \c1sid \end{20d04fe0-3aea-1069-a2d8-08002b30309d} \shell folder$ Opens key:

Opens key: HKCU\software\classes\clsid\{208d2c60-3aea-1069-a2d7-

08002b30309d}\shellfolder

HKCR\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder Opens key:

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

08002b30309d}\shellfolder

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

Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-42a0-1069-

a2ea-08002b30309d}

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

08002b30309d}\inprocserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32 $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows nt + current version + image file execution$ Opens key:

options\apphelp.dll

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

HKLM\software\microsoft\com3 Opens kev:

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

options\comres.dll

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

options\clbcatq.dll

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

Opens key: HKLM\software\classes

Opens key: HKCR\clsid

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

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

08002b30309d}\treatas

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

08002b30309d}\inprocserverx86

HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86 Opens key:

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

08002b30309d}\localserver32

HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32 Opens key:

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

08002b30309d}\inprochandler32

HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32 Opens key:

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

08002b30309d}\inprochandlerx86

Opens key:

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

08002b30309d}\localserver

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

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

options\ieframe.dll

Opens key: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe

Opens key: HKLM\software\microsoft\internet explorer\setup

Opens key: HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-

0000c05bae0b}\typelib

 $HKCR\interface \\ \{eab22ac1-30c1-11cf-a7eb-0000c05bae0b\} \\ typelib$ Opens key: Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}

HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba} Opens key: Opens key: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-

00aa00404770}\proxystubclsid32

Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32

Opens key: HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c82-

00aa004ba90b}\proxystubclsid32

HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32 Opens key:

Opens key: HKCU\software\classes\interface\{000214e6-0000-0000-c000-

00000000046}\proxystubclsid32

HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32 Opens key:

Opens key: HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-

00c04f79abd1}\proxystubclsid32

 $HKCR\interface \ \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\}\ proxystubclsid32$ Opens key:

Opens key: HKCU\software\classes\clsid\{11016101-e366-4d22-bc06-

4ada335c892b}\shellfolder

 $HKCR \ clsid \ \{11016101-e366-4d22-bc06-4ada335c892b\} \ shell folder$ Opens key:

Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{1f4de370 - d627 - 11d1 - ba4f - d627 - d$

00a0c91eedba}\shellfolder

 $HKCR\clsid\{1f4de370-d627-11d1-ba4f-00a0c91eedba}\shellfolder$ Opens key:

Opens key: HKCU\software\classes\clsid\{450d8fba-ad25-11d0-98a8-

0800361b1103}\shellfolder

 $HKCR \verb|\clsid| \{450d8fba-ad25-11d0-98a8-0800361b1103\} \verb|\shellfolder|$ Opens key:

Opens key: HKCU\software\classes\clsid\{645ff040-5081-101b-9f08-

00aa002f954e}\shellfolder

Opens key: $HKCR \ clsid \ \{645ff040-5081-101b-9f08-00aa002f954e\} \ shell folder$ Opens key: HKCU\software\classes\clsid\{e17d4fc0-5564-11d1-83f2-

00a0c90dc849}\shellfolder

HKCR\clsid\{e17d4fc0-5564-11d1-83f2-00a0c90dc849}\shellfolder Opens key:

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks Opens key: HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-

00c04fd91972}\inprocserver32

HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32 Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\app paths\cmd.exe Opens key: HKLM\software\microsoft\windows\currentversion\policies\associations $\label{thm:condition} \begin{tabular}{ll} HKCU \label{thm:conditions} \begin$ Opens key:

Opens key: HKCU\software\classes\.exe

Opens key: HKCR\.exe

HKCU\software\classes\.ade Opens key: Opens key: HKCR\.ade

Opens key: HKCU\software\classes\.adp

Opens kev: HKCR\.adn

Opens key: HKCU\software\classes\.app

Opens key: HKCR\.app

HKCU\software\classes\.asp Opens key:

Opens key: HKCR\.asp

Opens key: HKCU\software\classes\.bas

Opens key: HKCR\.bas

Opens key: HKCU\software\classes\.bat

Opens key: HKCR\.bat

HKCU\software\classes\.cer Opens key: Opens key: HKCR\.cer Opens key: HKCU\software\classes\.chm

HKCR\.chm Opens key:

Opens key: HKCU\software\classes\.cmd

HKCR\.cmd

Opens key:

HKCU\software\classes\.com Opens key:

Opens key: HKCR\.com HKCU\software\classes\.cpl

Opens key: Opens key: HKCR\.cpl

Opens key: HKCU\software\classes\.crt

HKCR\.crt Opens kev:

HKCU\software\classes\.csh Opens key:

Opens key: HKCR\.csh

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

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

00c04fb6bfc4}\treatas

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

00c04fb6bfc4}\inprocserver32

 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32$ Opens key:

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

00c04fb6bfc4}\inprocserverx86

 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\clsid$ Opens key:

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

00c04fb6bfc4}\localserver32

 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32$ Opens key:

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

00c04fb6bfc4}\inprochandler32

Opens key: $HKCR \clsid \footnote{Tb8a2d94-0ac9-11d1-896c-00c04fb6bfc4} \label{thkcr} Linprochamdler 32 \clsid \footnote{Tb8a2d94-0ac9-11d1-896c-00c04fb6bfc4} \label{thkcr}$

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

00c04fb6bfc4}\inprochandlerx86

 $HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\nprochandlerx86$ Opens key:

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

00c04fb6bfc4}\localserver

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000

Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-

a2d8-08002b30309d}

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

08002b30309d}\inprocserver32

Opens kev: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\setupapi.dll

HKLM\system\currentcontrolset\control\minint Opens key:

Opens key: HKLM\system\wpa\pnp

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

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

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume

Opens kev:

 $HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ mountpoints 2 \ cpc \ volume \ \ \{f90255c2-6bc4-f9025c2-6bc4-f$

11e3-9fc7-806d6172696f}\

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

Opens key: HKCR\drive\shellex\folderextensions

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \drive \shellex \folder extensions \fine \classes \drive \shellex \folder \end{tabular} \end{tabular}$ Opens key:

4442-804e-409d6c4515e9}

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

409d6c4515e9}

Opens kev: HKCU\software\classes\directory

Opens key: HKCR\directory

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

HKCR\directory\curver Opens key:

Opens key: HKCR\directory\

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

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

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

Opens key: HKCR\directory\clsid Opens key: HKCU\software\classes\folder

Opens key: HKCR\folder

HKCU\software\classes\folder\clsid Opens kev:

Opens key: HKCR\folder\clsid

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts $\label{thm:local_explorer} \begin{tabular}{ll} HKCU \end{tabular} software \end{tabular} in the constraint \end{tabular} in the constraint \end{tabular} and \end{tabular} in the constraint \end{tabular} in the constraint$ Opens key:

Opens key: HKCU\software\classes\exefile

Opens key: HKCR\exefile

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

Opens key: HKCR\exefile\curver Opens key: HKCR\exefile\

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

Opens key: HKCR\exefile\shellex\iconhandler

Opens key: HKCU\software\classes\systemfileassociations\.exe

Opens key: HKCR\systemfileassociations\.exe

Opens key: HKCU\software\classes\systemfileassociations\application

Opens key: HKCR\systemfileassociations\application HKCU\software\classes\exefile\clsid Opens key:

Opens key: HKCR\exefile\clsid Opens key: HKCU\software\classes*

HKCR* Opens key:

Opens key: HKCU\software\classes*\clsid

Opens key: HKCR*\clsid

HKCU\software\classes\exefile\shell Opens key:

Opens key: HKCR\exefile\shell

HKCU\software\classes\exefile\shell\open Opens key:

HKCR\exefile\shell\open Opens key:

Opens key: HKCU\software\classes\exefile\shell\open\command

HKCR\exefile\shell\open\command Opens kev:

Opens key:

HKCU\software\microsoft\windows\currentversion\policies\explorer\restrictrun HKCU\software\classes\exefile\shell\open\ddeexec Opens key:

Opens key: HKCR\exefile\shell\open\ddeexec

Opens key: HKCU\software\classes\applications\cmd.exe

Opens kev: HKCR\applications\cmd.exe

HKCU\software\microsoft\windows\shellnoroam Opens key:

Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache\

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

Opens key: HKLM\system\wpa\tabletpc Opens key: HKLM\system\wpa\mediacenter

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} approximately approxima$ Opens key:

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\cmd.exe

HKLM\software\microsoft\windows nt\currentversion\appcompatflags Opens key: Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects

Opens key: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths$

Opens key:

be2efd2c1a33}

Opens key:

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

Opens key:

edd5fbde1328}

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91}

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-

7c29ddecae3f} Opens kev:

085bcc18a68d} Opens key: b91490411bfc} Opens kev: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens kev: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens key: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 131072 \ paths$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones Opens key: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 262144 \ paths$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths Opens kev: Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \oline \oline \code identifiers \code \code \end{tabular} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code \cod$ Opens key: $HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 4096 \ paths$ Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens key: $HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 131072 \ paths$ Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones Opens key: $HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 262144 \ paths$ Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ explorer \verb+ shell folders + of the lemma of the lemma$ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cmd.exe Opens key: HKLM\software\microsoft\windows Opens key: HKLM\software\microsoft\windows\html help HKLM\software\microsoft\windows\help Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\acgenral.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\shimeng.dll

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

options\msacm32.dll

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

options\uxtheme.dll

HKLM\software\microsoft\audiocompressionmanager\drivercache Opens kev:

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus msacm.ima adpcmark to the compression manager \setminus driver cache \setminus driver ca$

Opens kev:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msadpc manager \setminus driver cache \setminus msadpc manager \setminus driver cache \setminus msadpc msa$

Opens kev: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711

Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610

Opens key: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ trspch$ Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723

Opens key:

```
Opens key:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. sl\_anet
```

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2 Opens key: Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm

Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm HKCU\software\microsoft\windows\currentversion\thememanager Opens key:

HKCU\software\policies\microsoft\windows\system Opens key: Opens key: HKLM\software\microsoft\command processor HKCU\software\microsoft\command processor Opens key: HKLM\system\currentcontrolset\control\nls\locale Opens key:

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

Opens key: HKLM\system\currentcontrolset\control\nls\language groups

HKLM\software\microsoft\windows Opens key: nt\currentversion\appcompatflags\custom\tasklist.exe

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

options\tasklist.exe

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

options\mpr.dll

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

options\framedyn.dll

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

options\dbghelp.dll

Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder

Opens key: HKLM\software\microsoft\wbem\cimom

Opens key: HKLM\software\microsoft\ctf\compatibility\tasklist.exe

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

options\tasklist.exe\rpcthreadpoolthrottle

Opens key: HKLM\svstem\currentcontrolset\control\lsa

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

options\xpsp2res.dll

HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24} Opens key:

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24} Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\treatas

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprocserver32

Opens key: $HKCR \ clsid \ \{4590f811-1d3a-11d0-891f-00aa004b2e24\} \ in procserver 32$

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprocserverx86

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86

HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-Opens kev:

00aa004b2e24}\localserver32

HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandler32

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32

HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-Opens kev:

00aa004b2e24}\inprochandlerx86

HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86 Opens key:

HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-Opens key:

00aa004b2e24}\localserver

 $\label{localserver} $HKCR\clsid\\{4590f811-1d3a-11d0-891f-00aa004b2e24}\\\localserver$ Opens key:

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

options\wbemcomn.dll

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

options\wbemprox.dll

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

options\winsta.dll

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820} Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\treatas

HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprocserver32

 $HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\inprocserver32$ Opens key:

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprocserverx86

HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserverx86 Opens key:

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\localserver32

 $HKCR \ clsid \ \{8bc3f05e-d86b-11d0-a075-00c04fb68820\} \ localserver 32$ Opens key:

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandler32

 $HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\tinprochandler32$ Opens key:

HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-Opens key:

00c04fb68820}\inprochandlerx86

 $HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\ \ inprochandlerx86$ Opens key:

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\localserver

Opens key: $\label{localserver} $HKCR\clsid{8bc3f05e-d86b-11d0-a075-00c04fb68820} \land calserver $$ $HKCR\cls$

```
HKCU \setminus software \setminus classes \setminus appid \setminus \{8bc3f05e-d86b-11d0-a075-00c04fb68820\}
    Opens key:
    Opens key:
                                                               HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
    Opens key:
                                                               HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
                                                               HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
    Opens key:
    Opens kev:
                                                               HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32
                                                              HKCR \land f309ad18-d86a-11d0-a075-00c04fb68820 \rbrace \land proxystubclsid32
    Opens key:
                                                               HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
    Opens key:
    Opens key:
                                                               HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
                                                               HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
    Opens key:
00aa004b2e24}\treatas
    Opens key:
                                                               \label{local-condition} HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\ \ treat as
    Opens key:
                                                               HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32
    Opens key:
                                                              HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
                                                               HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
    Opens key:
00aa004b2e24}\inprocserverx86
    Opens key:
                                                               HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86
    Opens key:
                                                               HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\localserver32
    Opens key:
                                                               HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32
    Opens key:
                                                               HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler32
    Opens key:
                                                               HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32
    Opens key:
                                                               HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandlerx86
    Opens key:
                                                               HKCR \ clsid \ \{7c857801-7381-11cf-884d-00aa004b2e24\} \ in prochandler x 86 \ in prochadler x 86 \ in prochandler x 86 \ in prochadler x 86 \ in prochad
    Opens key:
                                                              HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\localserver
    Opens key:
                                                               HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver
    Opens key:
                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemsvc.dll
    Opens key:
                                                               HKCU \setminus software \setminus classes \setminus interface \setminus \{d4781cd6 - e5d3 - 44df - ad94 - 930efe48a887\}
    Opens key:
                                                               HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
                                                               HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-
    Opens key:
930efe48a887}\proxystubclsid32
                                                              HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32
    Opens kev:
                                                               HKCU \setminus software \setminus classes \setminus interface \setminus \{9556dc99-828c-11cf-a37e-00aa003240c7\}
    Opens key:
    Opens key:
                                                               HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
    Opens key:
                                                               HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32
                                                               HKCR \land eface \land \{9556dc99-828c-11cf-a37e-00aa003240c7\} \land proxystubclsid32\} \land efactor for the proxystubcl in the proxystub of the proxystub of
    Opens key:
                                                               HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
    Opens kev:
                                                               HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
    Opens key:
                                                               HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
    Opens key:
ce99a996d9ea}\treatas
                                                               HKCR\clsid\\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\\\treatas
    Opens key:
```

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprocserver32

 $HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\ \ linprocserver 32$ Opens key: Opens kev:

HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprocserverx86

 $HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\ \ linprocserverx86a$ Opens key:

HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens key:

ce99a996d9ea}\localserver32

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver32

HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens kev:

ce99a996d9ea}\inprochandler32

 $HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\tinprochandler 32$ Opens key:

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprochandlerx86

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandlerx86

HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens key:

ce99a996d9ea}\localserver

HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver Opens key:

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

options\msvcp60.dll

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

options\wldap32.dll

Opens kev: HKLM\svstem\currentcontrolset\services\ldap

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

options\ntdsapi.dll

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

options\fastprox.dll

Opens key:

HKCR\interface\{027947e1-d731-11ce-a357-00000000001} Opens kev: Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-

000000000001}\proxystubclsid32

Opens key: HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32 Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd} Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\treatas

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserver32

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprocserverx86

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\localserver32

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver32

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandler32

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\inprochandlerx86

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-

00104b703efd}\localserver

Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver

 $Opens~key: \\ HKCU \setminus software \setminus \{1c1c45ee-4395-11d2-b60b-00104b703efd\}$

Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd\}
Opens key: HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-

00104b703efd}\proxystubclsid32

Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
Opens key: HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-

 $00104b703efd \} \ \ proxystubcl sid 32$

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[6b1383f452de6d7b6d9a656c24904858]

Queries value: HKLM\software\microsoft\windows nt\currentversion\ime

compatibility[6b1383f452de6d7b6d9a656c24904858]

Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]

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

manager[criticalsectiontimeout]

 $Queries \ value: \\ HKLM \ software \ microsoft \ ole[rwlockresourcetime out]$

Queries value: HKCR\interface[interfacehelperdisableall]

00000000046}[interfacehelperdisableall]

Queries value: HKCR\interface\{00020400-0000-0000-c000-

00000000046}[interfacehelperdisableallforole32]
Oueries value: HKCU\control panel\desk

Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]

manager[safeprocesssearchmode]

Queries value:

Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKLM\system\currentcontrol\set\control\nls\codepage[932]
Queries value: HKLM\system\currentcontrol\set\control\nls\codepage[949]

Queries value: HKLM\system\currentcontrol\set\control\nls\codepage[949]

Queries value: HKLM\system\currentcontrolset\control\nls\codepage[952]

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

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

Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]

Oueries value: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 1]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]

HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]

```
Oueries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
 Oueries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi81
 Oueries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
 Queries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
 Oueries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
 Queries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
 Oueries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
 Oueries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
 Oueries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
 Oueries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
 Oueries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
 Queries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
 Oueries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
 Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
 Queries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
 Oueries value:
 Queries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
 Queries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
 Oueries value:
 Queries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
 Queries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
 Oueries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
 Queries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
 Queries value:
                            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
 Oueries value:
                            HKLM\software\microsoft\rpc[maxrpcsize]
                            HKLM\system\currentcontrolset\services\disk\enum[0]
 Queries value:
 Queries value:
                            HKCU\control panel\desktop[smoothscroll]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableimprovedzonecheck]
                            HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[6b1383f452de6d7b6d9a656c24904858.exe]
 Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
                           HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
 Oueries value:
ab78-1084642581fb1
                            HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
 Queries value:
0000-0000000000000]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[secureprotocols]
                            HKLM\software\policies\microsoft\internet
 Queries value:
explorer\main[security_hklm_only]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[certificaterevocation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablekeepalive]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[cachemode]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablenegotiate]
                            \label{lem:hkcu} \verb+KCU\+software\+microsoft\+windows\+currentversion\+internet
 Queries value:
settings[disablebasicoverclearchannel]
 Queries value:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
                           HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[clientauthbuiltinui]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache[signature]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
                           \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
 Oueries value:
settings\5.0\cache\content[peruseritem]
 Queries value:
                            HKLM\system\setup[systemsetupinprogress]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\explorer\user shell
```

folders[cache]

```
Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
settings\5.0\cache\content[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\cookies[peruseritem]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\cookies[cachelimit]
                          \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
 Queries value:
settings\5.0\cache\history[peruseritem]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\history[peruseritem]
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[history]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\history[cachelimit]
 Queries value:
HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
 Queries value:
                          settings\5.0\cache\extensible cache\ietld[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} internet \\ \end{tabular}
 Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
 Queries value:
                          settings\5.0\cache\extensible cache\ietld[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
 Queries value:
                          settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
```

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

Queries value:

```
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                           \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\5.0\cache\extensible cache\privacie:[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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]
                           \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\5.0\cache\extensible cache\privacie:[cacheoptions]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
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]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[connectretries]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[receivetimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[httpdefaultexpirytimesecs]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
 Oueries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[6b1383f452de6d7b6d9a656c24904858.exe]
 Queries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablecachingofsslpages]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablent4rascheck]
```

```
Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[sendextracrlf]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypassftptimecheck]
                           \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[releasesocketduringauth]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[releasesocketduring401auth]
                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[releasesocketduring401auth]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[wpadsearchalldomains]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablelegacypreauthasserver]
                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablelegacypreauthasserver]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasshttpnocachecheck]
  Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
  Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[headerexclusionlistforcache]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dnscachetimeout]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnonzonecrossing]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertsending]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpostredirect]
  Queries value:
                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[alwaysdrainonredirect]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonhttpstohttpredirect]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000003 \ [packed catalog item]
  Queries value:
```

Queries value:

```
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (000000000005 [packed catalog item]) \ details \ d
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000006[packedcatalogitem]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (000000000007 [packed catalog item]) \ details \ d
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000009[packedcatalogitem]
   Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 000000000001[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[supported name space]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ (0000000000001[enabled]) \ and \ (enabled) \ and \ (enable
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap amespace\_catalog \\ S \setminus catalog\_entries \setminus 00000000000002[providerid]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000002 \ [address family]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
   Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ 0000000000002 \ [version]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000002[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[displaystring]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap amespace\_catalog \\ S \setminus catalog\_entries \setminus 0000000000003[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo]
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2 32numhandlebuckets]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
                                                     HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[globaluseroffline]
   Oueries value:
                                                     HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
   Queries value:
                                                      HKLM\software\microsoft\windows\currentversion\internet
```

settings[truncatefilename] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[badproxyexpirestime] Queries value:

HKCU\software\microsoft\windows\currentversion\internet

Oueries value:

Oueries value:

settings[urlencoding]

 $HKLM \ software \ microsoft \ windows \ current version \ telephony \ [tapi32 requestre try time out]$

HKLM\software\microsoft\tracing[enableconsoletracing] Oueries value: HKLM\software\microsoft\tracing\rasapi32[enablefiletracing] Oueries value: HKLM\software\microsoft\tracing\rasapi32[filetracingmask] Oueries value: HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing] Queries value: Oueries value: HKLM\software\microsoft\tracing\rasapi32[consoletracingmask] Queries value: HKLM\software\microsoft\tracing\rasapi32[maxfilesize] Oueries value: HKLM\software\microsoft\tracing\rasapi32[filedirectory] Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common appdata] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[userenvdebuglevel] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[chkaccdebuglevel] HKLM\system\currentcontrolset\control\productoptions[producttype] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[personal] HKCU\software\microsoft\windows\currentversion\explorer\user shell Oueries value: folders[local settings] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsopdebuglevel] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[profilesdirectory] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[allusersprofile] HKLM\software\microsoft\windows Queries value: nt\currentversion\profilelist[defaultuserprofile] HKLM\software\microsoft\windows\currentversion[programfilesdir] Queries value: Oueries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileimagepath] HKCU\software\microsoft\windows Queries value: nt\currentversion\winlogon[parseautoexec] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[migrateproxy] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyenable] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyserver] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxvoverride] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[autoconfigurl] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\connections[savedlegacysettings] Queries value: $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\$ settings\connections[defaultconnectionsettings] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[6b1383f452de6d7b6d9a656c24904858.exe] HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_mime_handling[*] HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Queries value: Oueries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow] Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh] HKLM\software\policies\microsoft\internet Oueries value: 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 Queries value: settings\zones\2[flags] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\4[flags] Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[6b1383f452de6d7b6d9a656c24904858.exe] Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[*] Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[6b1383f452de6d7b6d9a656c24904858.exe] Queries value: ${\tt HKLM \backslash software \backslash microsoft \backslash internet}$ explorer\main\featurecontrol\feature_localmachine_lockdown[*] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[createuricachesize] HKLM\software\microsoft\windows\currentversion\internet

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

HKLM\software\microsoft\windows\currentversion\internet

Oueries value:

Queries value:

Queries value:

settings[createuricachesize]

settings[enablepunvcode]

```
settings[enablepunycode]
                         HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zonemap[autodetect]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
 Queries 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[filterclusterip]
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
                         \label{lem:hklm} \verb+Kklm \system \current control set \services \dnscache \parameters [use hosts file]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Queries value:
HKLM \backslash system \backslash current control set \backslash services \backslash tcpip \backslash parameters [enable adapter domain name registration]
 Queries value:
HKLM \ system \ current control set \ services \ dns cache \ parameters \ [register reverse lookup]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetop]eveldomainzones]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [server priority time limit]
 Queries value:
```

```
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
                                                        HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
    Queries value:
    Queries value:
c7d49d7cecdc}[enabledhcp]
    Oueries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[leaseobtainedtime]
    Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr
c7d49d7cecdc}[leaseterminatestime]
    Queries value:
c7d49d7cecdc}[dhcpserver]
                                                        HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
    Queries value:
    Queries value:
                                                        HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
    Queries value:
c7d49d7cecdc}[queryadaptername]
c7d49d7cecdc}[disableadapterdomainname]
c7d49d7cecdc}[registrationenabled]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
    Queries value:
c7d49d7cecdc}[registrationmaxaddresscount]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[maxnumberofaddressestoregister]
    Oueries value:
c7d49d7cecdc}[domain]
    Queries value:
HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4303-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-abe3-4300-a
c7d49d7cecdc}[dhcpdomain]
    Oueries value:
c7d49d7cecdc}[ipautoconfigurationenabled]
    Queries value:
c7d49d7cecdc}[addresstype]
    Oueries value:
c7d49d7cecdc}[nameserver]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
                                                         HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
    Queries value:
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
                                                        HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
    Oueries value:
cryptographic provider[type]
    Queries value:
                                                        HKLM \ software \ microsoft \ strong
cryptographic provider[image path]
                                                        HKLM\software\microsoft\rpc\securityservice[10]
    Oueries value:
    Queries value:
                                                        HKLM\software\microsoft\cryptography[machineguid]
    Oueries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
    Queries value:
                                                        HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
    Queries value:
HKLM\system\currentcontrol\set\control\lsa\sspicache\msapsspc.dll[comment]
    Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
                                                        HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
    Oueries value:
    Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
```

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]

Queries value: Queries value:

```
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
                                                                    HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
     Oueries value:
     Oueries value:
                                                                    HKLM\system\currentcontrolset\services\winsock\parameters[transports]
     Queries value:
                                                                    HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
     Oueries value:
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
     Queries value:
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
     Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
     Queries value:
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
     Oueries value:
     Oueries value:
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
     Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
     Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
     Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
     Queries value:
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
     Oueries value:
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
     Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
                                                                   \label{lem:hklm} \verb+Kklm \+ system \+ control \+ lsa \+ spicache \+ msnsspc.dll[rpcid]
     Queries value:
     Queries value:
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
     Queries value:
                                                                    HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
     Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
     Queries value:
                                                                    HKLM\system\currentcontrolset\services\netbt\linkage[export]
                                                                    HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
     Queries value:
                                                                    HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]
     Queries value:
     Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
     Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
     Queries value:
HKCU \ software \ microsoft \ windows \ current version \ policies \ \ explorer [no common groups]
HKLM \ software \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{11016101-e366-4d22-e4d22-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-e4d24-
bc06-4ada335c892b}[suppressionpolicy]
ba4f-00a0c91eedba}[suppressionpolicy]
98a8-0800361b1103}[suppressionpolicy]
     Oueries value:
HKLM \label{eq:hkkm} Lose the last of th
9f08-00aa002f954e}[suppressionpolicy]
HKLM \ software \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564-11d1-e17d4fc0-5564
83f2-00a0c90dc849}[suppressionpolicy]
                                                                    HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
     Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
     Oueries value:
                                                                    HKCR\clsid\{208d2c60-3aea-1069-a2d7-
 08002b30309d}\shellfolder[wantsparsedisplayname]
    Queries value:
                                                                   HKCR\clsid\{871c5380-42a0-1069-a2ea-
 08002b30309d}\shellfolder[wantsparsedisplayname]
                                                                    HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
     Queries value:
     Queries value:
                                                                   HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
                                                                    HKLM\software\microsoft\windows\currentversion\shell
     Oueries value:
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
    Queries value:
                                                                   \label{local-objective} \verb|HKCU\software\microsoft\windows\currentversion\shell| \\
 extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
     Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
                                                                    HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}}
0x401]
     Queries value:
                                                                    \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \shell
extensions \\ \\ cached [\{871c5380-42a0-1069-a2ea-08002b30309d\} \\ \\ \{000214e6-0000-0000-c000-0000000000046\} \\ \\ \\ \\ extensions \\ \\ \\ extensions \\ \\ extensio
0x4011
                                                                    HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
     Oueries value:
                                                                   HKLM\software\microsoft\com3[com+enabled]
     Queries value:
                                                                    HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
     Oueries value:
                                                                    HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
     Queries value:
                                                                    HKLM\software\microsoft\com3[regdbversion]
```

```
HKCR\clsid\{871c5380-42a0-1069-a2ea-
 Oueries value:
08002b30309d}\inprocserver32[inprocserver32]
                         HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
 Oueries value:
 Queries value:
                         HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
 Oueries value:
                         HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
                         HKLM\software\microsoft\internet
 Oueries value:
explorer\setup[iexplorelastmodifiedhigh]
                         HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
 Oueries value:
 Oueries value:
                         HKLM\software\microsoft\internet explorer\setup[installstarted]
 Queries value:
                         HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
 Oueries value:
                         HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
                         HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[]
 Oueries value:
 Queries value:
                         HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32[]
 Queries value:
                         HKCR\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[wantsparsedisplayname]
                         HKCR\clsid\{1f4de370-d627-11d1-ba4f-
 Queries value:
00a0c91eedba}\shellfolder[wantsparsedisplayname]
                        HKCR\clsid\{450d8fba-ad25-11d0-98a8-
 Oueries value:
0800361b1103}\shellfolder[wantsparsedisplayname]
 Queries value:
                         HKCR\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[wantsparsedisplayname]
                         HKCR\clsid\{e17d4fc0-5564-11d1-83f2-
 Queries value:
00a0c90dc849}\shellfolder[wantsparsedisplayname]
                        HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
 Queries value:
                         HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
 Queries value:
00c04fd91972}\inprocserver32[loadwithoutcom]
                        HKCR\.exe[]
 Oueries value:
                         HKCR\.asp[]
 Queries value:
 Queries value:
                         HKCR\.bat[]
                        HKCR\.cer[]
 Queries value:
                         HKCR\.chm[]
 Queries value:
 Queries value:
                         HKCR\.cmd[]
                         HKCR\.com[]
 Oueries value:
                         HKCR\.cpl[]
 Queries value:
                         HKCR\.crt[]
 Oueries value:
                         HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
 Oueries value:
00c04fb6bfc4}\inprocserver32[inprocserver32]
                         HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
 Queries value:
 Oueries value:
                         HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
                         HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
 Queries value:
00c04fb6bfc4}\inprocserver32[threadingmodel]
 Queries value:
                        HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
                        HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[specialfolderscachesize]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1806]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\nprocserver32[]
 Queries value:
                         HKLM\system\wpa\pnp[seed]
 Oueries value:
 Queries value:
                         HKLM\system\setup[osloaderpath]
 Oueries value:
                         HKLM\system\setup[systempartition]
                         HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Oueries value:
 Oueries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
 Queries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus setup [service pack cachepath]
                         HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion[devicepath]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\setup[loglevel]
                         HKLM\software\microsoft\windows\currentversion\setup[logpath]
 Queries value:
11e3-9fc7-806d6172696f}[data]
 Oueries value:
11e3-9fc7-806d6172696f}[generation]
                         HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
 Oueries value:
409d6c4515e9}[drivemask]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [force active desktop on] \\
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
```

Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu] HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Oueries value: Oueries value: $HKCU \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'advanced [showcompcolor]$ Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter] Queries value: Queries value: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [show superhidden]$ HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling] HKCR\directory[docobject] Oueries value: HKCR\directory[browseinplace] Queries value: HKCR\directory[isshortcut] Queries value: Queries value: HKCR\directory[alwaysshowext] Oueries value: HKCR\directory[nevershowext] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions] Oueries value: HKCR\exefile[docobject] HKCR\exefile[browseinplace] Queries value: HKCR\exefile[isshortcut] Queries value: Oueries value: HKCR\exefile[alwaysshowext] HKCR\exefile[nevershowext] Queries value: HKCR\exefile\shell[] Oueries value: Queries value: HKCR\exefile\shell\open\command[] HKCR\exefile\shell\open\command[command] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[flags] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[state] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[userpreference] HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Oueries value: 1757981266-507921405-1957994488-1003[centralprofile] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileloadtimelow] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileloadtimehigh] HKCU\software\microsoft\windows\shellnoroam\muicache[langid] Oueries value: Oueries value: $HKCU \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus muicache [c: \windows \setminus system 32 \setminus cmd.exe]$ Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun] Oueries value: $\label{thm:local_continuous} \begin{tabular}{l} HKCU \software \mbox{$\mbox{$m$icrosoft}$ windows \current version \policies \explorer[disallow run] \end{tabular}$ Queries value: $HKCU \ software \ microsoft \ windows \ current version \ policies \ (explorer [noruna sin stall prompt]) \ descriptions \ for the prompt \$ Queries value: HKLM\system\wpa\mediacenter[installed] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled] HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels] Oueries value: Oueries value: be2efd2c1a33}[itemdata] Oueries value: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ paths \ \{dda3f824-d8cb-441b-834d-d8cb-441b$

 $Queries\ value: \\ HKLM\ software\ policies\ microsoft\ windows\ safer\ code identifiers\ 0\ hashes\ \{349d35ab-37b5-462f-9b89-4666-9b89-46666-9b89-4666-9b89-4666-9b89-4666-9b89-4666-9b89-4666-9b89-4666-9b89-4666-9b8$

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-

be2efd2c1a33}[saferflags]

edd5fbde1328}[itemdata]

Oueries value:

edd5fbde1328}[hashalg]

Queries value:

Queries value:

Oueries value:

Oueries value:

Oueries value:

Queries value:

Queries value:

Oueries value:

Queries value:

Oueries value:

Queries value:

Queries value:

Queries value:

Queries value:

Queries value:

 $HKLM \ software \ bolicies \ icrosoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} [item data]$

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} \ [hashalg]$

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} [itemsize]$

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} \ [saferflags]$

Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [default level]$

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]

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

folders[cache]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]

Queries value: HKCU\software\microsoft\visual basic\6.0[allowunsafeobjectpassing]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cmd]

Queries value: HKCU\software\microsoft\multimedia\audio[systemformats]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.imaadpcm]

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
 Oueries value:

 $HKLM \verb|\software\microsoft\audiocompression manager \verb|\drivercache\msacm.imaadpcm[cfiltertags]| \\$

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msadpcm]

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]

Queries value:

 $HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox{|} msadpcm[cformattags]|$

Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags] HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msg711] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags] Oueries value: $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. msg 711 [a formattag cache]$ Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msg711[cfilter tags]$ HKLM\software\microsoft\windows Queries value: nt\currentversion\drivers32[msacm.msgsm610] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport] Oueries value: $\label{thm:macmmag} \begin{tabular}{ll} HKLM \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} microsoft \end{tabular} audio compression manager \end{tabular} driver cache \end{tabular} macm. msgsm610 [cformattags] \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} \begin{tabular}{ll} for each end of the compressi$ HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags] HKLM\software\microsoft\windows Queries value: nt\currentversion\drivers32[msacm.trspch] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg723] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags] Oueries value: $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. msg 723 [a formattag cache]$ Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \\ msg723[cfilter tags]$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msaudio1] Oueries value: Oueries value: $HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. msaudio1[cformattags]$ Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msaudio1 \lceil aformattag cache \rceil$ Queries value: $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msaudio1[cfilter tags]$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.sl_anet] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport] Oueries value: $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. sl_anet [cformattags]$ Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[cfiltertags] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport] Oueries value: Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.iac2[aformattag cache]$ HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.13acm[fdwsupport] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags] Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]

HKCU\software\microsoft\multimedia\audio compression

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} I3 acm [cfilter tags] \\$

Queries value:

Queries value:

```
manager\msacm[nopcmconverter]
                          HKCU\software\microsoft\multimedia\audio compression manager\priority
 Oueries value:
v4.00[priority1]
                          HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
 Queries value:
 Oueries value:
                          HKCU\control panel\desktop[lamebuttontext]
 Queries value:
                          HKLM\software\microsoft\command processor[disableunccheck]
                          HKLM\software\microsoft\command processor[enableextensions]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\command processor[delayedexpansion]
 Oueries value:
                          HKLM\software\microsoft\command processor[defaultcolor]
 Oueries value:
                          HKLM\software\microsoft\command processor[completionchar]
 Oueries value:
                          HKLM\software\microsoft\command processor[pathcompletionchar]
 Queries value:
                          HKLM\software\microsoft\command processor[autorun]
 Oueries value:
                          HKCU\software\microsoft\command processor[disableunccheck]
                          \label{local-operator} \mbox{HKCU\software\mbox{\tt microsoft\command} processor[enable extensions]}
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\command processor[delayedexpansion]
 Queries value:
                          HKCU\software\microsoft\command processor[defaultcolor]
 Oueries value:
                          HKCU\software\microsoft\command processor[completionchar]
 Queries value:
                          HKCU\software\microsoft\command processor[pathcompletionchar]
 Oueries value:
                          HKCU\software\microsoft\command processor[autorun]
                          HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\compatibilitv32\ftasklist1
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[tasklist]
                          HKLM\software\microsoft\wbem\cimom[logging]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[logging directory]
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[log file max size]
                          HKLM\software\microsoft\ole[maximumallowedallocationsize]
 Oueries value:
 Queries value:
                          HKLM \setminus system \setminus current control \setminus lsa[everyone includes an onymous]
 Queries value:
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
 Queries value:
 Queries value:
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-
 Oueries value:
00aa004b2e24}\inprocserver32[threadingmodel]
                          HKLM\software\microsoft\wbem\cimom[repository directory]
 Oueries value:
                          HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
 Oueries value:
 Queries value:
                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[dllsurrogate]
 Queries value:
                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
                          HKCR \land f309 ad 18-d86 a-11 d0-a075-00 c04 fb68820 \rbrace \land proxystubclsid 32[]
 Oueries value:
                          HKCR\clsid\{7c857801-7381-11cf-884d-
 Queries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
 Queries value:
                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
 Oueries value:
                          HKCR\clsid\{7c857801-7381-11cf-884d-
 Queries value:
00aa004b2e24}\inprocserver32[threadingmodel]
 Queries value:
                          HKCR \ interface \ \{d4781cd6-e5d3-44df-ad94-930efe48a887\} \ proxystubclsid32[]
                          HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
 Oueries value:
 Queries value:
                         HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
 Oueries value:
 Oueries value:
                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
                          HKCR\clsid\{d68af00a-29cb-43fa-8504-
 Queries value:
ce99a996d9ea}\inprocserver32[threadingmodel]
 Queries value:
                          HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
                          HKLM\software\microsoft\wbem\cimom[processid]
 Oueries value:
                          HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
 Queries value:
 Oueries value:
                          HKLM\software\microsoft\wbem\cimom[contextlimit]
                          HKLM\software\microsoft\wbem\cimom[objectlimit]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[identifierlimit]
 Oueries value:
                          HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32[]
                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
 Queries value:
00104b703efd}\inprocserver32[inprocserver32]
                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
 Oueries value:
                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[appid]
 Oueries value:
 Queries value:
                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
 Queries value:
                          HKCR \ interface \ \{1c1c45ee-4395-11d2-b60b-00104b703efd\} \ proxystubclsid32[]
                          Oueries value:
 Value changes:
                          HKLM\software\microsoft\cryptography\rng[seed]
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
 Value changes:
folders[cache]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[history]
 Value changes:
                          HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common appdata]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
                          HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
```

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]

Value changes:

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ \{f90255c2-6bc4-11e3-9fc7-16bc4-16bc$

806d6172696f}[baseclass]