# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3332, Task ID: 836

Task ID: 836 Risk Level: 10

Date Processed: 2016-05-18 10:44:22 (UTC)

Processing Time: 28.88 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\1bb90eca6f10f100c1d941d1fe06e7a9.exe"

Sample ID: 3332 Type: basic Owner: admin

Label: 1bb90eca6f10f100c1d941d1fe06e7a9

Date Added: 2016-05-18 10:30:52 (UTC)

File Type: PE32:win32:gui File Size: 61440 bytes

MD5: 1bb90eca6f10f100c1d941d1fe06e7a9

SHA256: 85349ac8d14cdc29e66a07cda3c2bd0c128428825ffbc03fd0a90dddad2f15b5

Description: None

## Pattern Matching Results

3 Long sleep detected

6 Checks task list from command line

10 Creates malicious events: Beebone [Trojan]

4 Terminates process under Windows subfolder

### Process/Thread Events

Creates process: C:\WINDOWS\Temp\1bb90eca6f10f100c1d941d1fe06e7a9.exe

["c:\windows\temp\1bb90eca6f10f100c1d941d1fe06e7a9.exe" ]

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

tasklist&&del 1bb90eca6f10f100c1d941d1fe06e7a9.exe]

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

Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Terminates process: C:\WINDOWS\Temp\1bb90eca6f10f100c1d941d1fe06e7a9.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:

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

settings!temporary internet files!content.ie5!

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

settings!history!history.ie5!

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

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

Creates mutex: \BaseNamedObjects\SHIMLIB\_LOG\_MUTEX

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

Creates semaphore: \BaseNamedObjects\C:?WINDOWS?TEMP?1BB90ECA6F10F100C1D941D1FE06E7A9.EXE
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}

#### File System Events

Opens: C:\WINDOWS\Prefetch\1BB90ECA6F10F100C1D941D1FE06E-11DB81DB.pf

Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\msvbvm60.dl1
Opens: C:\WINDOWS\system32\imm32.dl1
Opens: C:\WINDOWS\system32\rpcss.dl1
Opens: C:\WINDOWS\system32\MSCTF.dl1
Opens: C:\WINDOWS\system32\sxs.dl1
Opens: C:\WINDOWS\system32\MSCTFIME.IME

Opens: C:\WINDOWS\Temp\1bb90eca6f10f100c1d941d1fe06e7a9.exe

```
C:\
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\WindowsShell.Config
                         C:\WINDOWS\system32\wininet.dll.123.Manifest
 Opens:
 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
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
 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:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Cookies
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
 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\winmm.dll
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 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\msv1_0.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
 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:
 Opens:
                         C:\WINDOWS\AppPatch
                         {\tt C:\WINDOWS\system32\wbem}
 Opens:
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
 Opens:
                         C:\WINDOWS\WINHELP.INI
                         C:\WINDOWS\WinSxS
 Opens:
 Opens:
                         C:\WINDOWS\system32\ntdll.dll
 Opens:
                         C:\WINDOWS\system32\kernel32.dll
 Opens:
                         C:\WINDOWS\system32\unicode.nls
 Opens:
                         C:\WINDOWS\system32\locale.nls
 Opens:
                         C:\WINDOWS\system32\sorttbls.nls
```

C:\WINDOWS\system32\msvcrt.dll

Opens:

C:\WINDOWS\system32\user32.dll Opens: Opens: C:\WINDOWS\system32\gdi32.dll C:\WINDOWS\system32\shimeng.dll Opens: Opens: C:\WINDOWS\AppPatch\AcGenral.dll Opens: C:\WINDOWS\system32\advapi32.dll Opens: C:\WINDOWS\system32\rpcrt4.dll Opens: C:\WINDOWS\system32\secur32.dll Opens: C:\WINDOWS\system32\ole32.dll Opens: C:\WINDOWS\system32\oleaut32.dll Opens: C:\WINDOWS\system32\msacm32.dll Opens: C:\WINDOWS\svstem32\version.dll Opens: C:\WINDOWS\system32\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:\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 Opens: C:\WINDOWS\system32\wbem\wbemprox.dll Opens: C:\WINDOWS\system32\wbem\wbemcomn.dll C:\WINDOWS\system32\winsta.dll Opens: 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

Reads from: C:\WINDOWS\Temp\1bb90eca6f10f100c1d941d1fe06e7a9.exe

Reads from: C:\AUT0EXEC.BAT

Reads from: C:\WINDOWS\system32\drivers\etc\hosts
Reads from: C:\WINDOWS\system32\rsaenh.dl1

Reads from: C:\WINDOWS\Registration\R00000000007.clb
Reads from: C:\WINDOWS\system32\cmd.exe

Reads from: C:\WINDOWS\System32\Cind.exe

Reads from: C:\winbows\Prefetch\CMD.EXE-08/B4001.p

#### **Network Events**

DNS query: domai.2noip.com

DNS response: domai.2noip.com  $\Rightarrow$  141.8.224.93 Connects to: 141.8.224.93:443

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

 $\label{lem:creates} Creates \ key: \\ HKLM \ software \ microsoft \ windows \ current version \ explorer \ shell \ folders$ 

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

settings\connections

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

awareness

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

Creates key:

Creates key:

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

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

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]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\1bb90eca6f10f100c1d941d1fe06e7a9.exe

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

Opens key:  $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$ 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\currentcontrolset\control\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 kev: 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

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

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:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre\_initialize$ Opens key:  $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus compatibility 32$ 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∖

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

HKLM\software\microsoft\ole Opens key:

Opens kev: HKCR\interface

HKCR\interface\{00020400-0000-0000-c000-00000000046} Opens key:

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

Opens key: HKCU\

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

HKCU\control panel\desktop Opens kev:

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

options\msctf.dll

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus 1bb 90eca 6f 10f 100c 1d 941d 1f e 06e7a 9. execute the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 1bb 90eca 6f 10f 100c 1d 941d 1f e 06e7a 9. execute the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 1bb 90eca 6f 10f 100c 1d 941d 1f e 06e7a 9. execute the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 1bb 90eca 6f 10f 100c 1d 941d 1f e 06e7a 9. execute the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 1bb 90eca 6f 10f 100c 1d 941d 1f e 06e7a 9. execute the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 1bb 90eca 6f 10f 100c 1d 941d 1f e 06e7a 9. execute the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 1bb 90eca 6f 10f 100c 1d 941d 1f e 06e7a 9. execute the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 1bb 90eca 6f 10f 100c 1d 941d 1f e 06e7a 9. execute the software \setminus microsoft \setminus ctf \setminus compatibility \setminus 1bb 90eca 6f 10f 100c 1d 941d 1f e 06e7a 9. execute the software \setminus microsoft \setminus ctf \setminus c$ 

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

options\version.dll

Opens key:  $\label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \mbox{$\mathbb{N}$ irrestriction} approximately ags \layers \end{tabular}$ Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

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

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

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

Opens kev: HKLM\svstem\currentcontrolset\services\disk\enum

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

options\shlwapi.dll

HKLM\software\microsoft\windows\currentversion\explorer\performance Opens kev: 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 kev:

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

Opens kev: 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

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

options\wininet.dll

Opens kev: HKCU\software\classes\

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

Opens key: HKCR\protocols\name-space handler

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

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

settings

Opens kev: HKI M\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\

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

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

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature\_ignore\_policies\_zonemap\_if\_esc\_enabled\_kb918915 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings\zonemap\domains\

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

settings\zonemap\domains\

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

settings\zonemap\ranges\

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

settings\zonemap\ranges\

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_unc\_savedfilecheck HKLM\software\microsoft\internet Opens key: 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 HKCU\software\policies Opens kev: HKCU\software Opens key: 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 kev:

HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\cookies

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

settings\5.0\cache\cookies HKCU\software\microsoft\windows\currentversion\internet

Opens key:

settings\5.0\cache\history HKLM\software\microsoft\windows\currentversion\internet Opens kev:

settings\5.0\cache\history

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

Opens key: HKLM\software\microsoft\rpc

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

options\1bb90eca6f10f100c1d941d1fe06e7a9.exe\rpcthreadpoolthrottle HKLM\software\policies\microsoft\windows nt\rpc Opens kev: Opens key: HKLM\system\currentcontrolset\control\computername

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

Opens key: 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 key:
settings\5.0\cache\extensible cache\iecompat
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\ietld
 Opens key:
                         \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\mshist012014033120140407
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\extensible cache\mshist012014041220140413
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                        HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                         HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                         \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
 Opens key:
settings\5.0\cache
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                         HKCU\software\microsoft\internet
 Opens key:
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
                        HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
                        HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                        HKLM\software\microsoft\internet
explorer \verb|\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
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                         HKLM\software\microsoft\internet
 Opens key:
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 kev:
                         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:
                         \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\ws2_32.dll
 Opens kev:
                         HKLM\svstem\currentcontrolset\services\winsock2\parameters
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
 Opens key:
Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens key:
Opens key:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
 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\00000000011
 Opens key:
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 key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
Opens key:
HKCU\software\microsoft\windows\currentversion\internet settings\wpad
 Opens key:
 Opens key:
                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                      HKLM\software\microsoft\internet
 Opens kev:
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
 Opens kev:
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
                      \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
 Opens key:
options\rasman.dll
 Opens key:
                      \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\rtutils.dll
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens kev:
options\winmm.dll
 Opens kev:
                      HKLM\software\microsoft\windows nt\currentversion\drivers32
 Opens key:
Opens key:
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
 Opens key:
                      HKLM\software\microsoft\windows\currentversion\telephony
                      HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
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
                      HKLM\software\microsoft\windows nt\currentversion\profilelist
 Opens key:
 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 kev:
1757981266-507921405-1957994488-1003
 Opens kev:
                      HKCU\environment
 Opens key:
                      HKCU\volatile environment
 Opens key:
                      \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\sensapi.dll
                      HKCU\software\microsoft\windows\currentversion\internet settings\http
 Opens kev:
filters\rpa
 Opens key:
                      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
                      HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
```

 $\begin{tabular}{ll} explorer $$ explorer \rightarrow $$ explorer \rightarrow$ 

HKCU\software\microsoft\internet

HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_mime\_handling

Opens key:

Opens key:

```
Opens key:
                           HKLM\software\microsoft\windows nt\currentversion\image file execution
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
 Opens key:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\protocoldefaults\
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
 Opens key:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                           HKI M\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\domains\msn.com
 Opens key:
                           HKLM\software\microsoft\windows\currentversion\internet
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 kev:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                           HKCU\software\microsoft\internet explorer\ietld
                           HKLM\software\policies\microsoft\internet explorer\security
 Opens key:
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
 Opens key:
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
 Opens key:
                           HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\0
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\0
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
 Opens kev:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\2
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
                           HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\3
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\3
 Opens key:
                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                           HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zones\4
 Opens key:
                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown
                           HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecon
                          trol\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\
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Opens key:
settings\lockdown_zones\
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\0
 Opens key:
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\0
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\1
 Opens key:
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\1
 Opens key:
                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
                           HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\2
 Opens key:
                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
```

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

settings\lockdown\_zones\2

Opens key:

```
settings\lockdown_zones\2
     Opens kev:
                                                                                         HKCU\software\microsoft\windows\currentversion\internet
 settings\lockdown_zones\3
                                                                                         HKLM\software\policies\microsoft\windows\currentversion\internet
     Opens key:
settings\lockdown_zones\3
                                                                                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \label{lem:hkcu} software \policies \microsoft \windows \current version \parelines \par
     Opens key:
 settings\lockdown_zones\3
     Opens key:
                                                                                         HKCU\software\microsoft\windows\currentversion\internet
 settings\lockdown_zones\4
      Opens key:
                                                                                         HKLM\software\policies\microsoft\windows\currentversion\internet
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
      Opens key:
                                                                                         HKLM\software\microsoft\internet
 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
                                                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
      Opens kev:
 options\iphlpapi.dll
      Opens key:
                                                                                          HKLM\system\currentcontrolset\services\tcpip\linkage
      Opens key:
                                                                                          HKLM\system\currentcontrolset\services\tcpip\parameters\
      Opens key:
                                                                                          HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
      Opens key:
                                                                                          HKLM\system\currentcontrolset\services\netbt\parameters
      Opens kev:
c7d49d7cecdc}
      Opens key:
                                                                                          HKLM\software\microsoft\rpc\securityservice
      Opens key:
                                                                                          HKLM\system\currentcontrolset\control\securityproviders
      Opens key:
                                                                                          HKLM\system\currentcontrolset\control\lsa\sspicache
      Opens key:
                                                                                          HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
      Opens key:
                                                                                          HKLM\software\policies\microsoft\system\dnsclient
      Opens key:
                                                                                          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll
      Opens key:
                                                                                          HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
      Opens key:
                                                                                          HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
      Opens key:
                                                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msv1_0.dll
      Opens key:
                                                                                          HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong
cryptographic provider
                                                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
      Opens key:
 options\rsaenh.dll
      Opens key:
                                                                                          HKLM\software\policies\microsoft\cryptography
                                                                                          HKLM\software\microsoft\cryptography
      Opens key:
      Opens key:
                                                                                          HKLM\software\microsoft\cryptography\offload
      Opens key:
                                                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\hnetcfg.dll
      Opens key:
                                                                                          HKLM\system\currentcontrolset\services\winsock\parameters
      Opens key:
                                                                                          HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
      Opens key:
                                                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
     Opens kev:
HKLM \ software \ `microsoft \ 'windows \ 'current version's hell compatibility \ 'applications' \ '1bb90eca \ '6f10f100c1d941d1fe06e7a9.exe' \ 'current \ 'version's hell \ 'vers
                                                                                          HKCU\software\microsoft\windows\currentversion\explorer
      Opens key:
      Opens key:
                                                                                          HKLM\software\microsoft\windows\currentversion\explorer
                                                                                          HKLM\software\microsoft\windows\currentversion\policies\explorer
      Opens key:
      Opens key:
                                                                                          HKCU\software\microsoft\windows\currentversion\policies\explorer
      Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace
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}
      Opens kev:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus desktop \setminus names pace \setminus \{1f4 de370 - d627 - 11d1 - d627 - 
ba4f-00a0c91eedba}
      Opens key:
HKLM \setminus software \setminus irrosoft \setminus ir
98a8-0800361b1103}
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{645ff040-5081-101b-
9f08-00aa002f954e}
      Opens key:
83f2-00a0c90dc849}
      Opens kev:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace
      Opens key:
                                                                                         HKCU\software\microsoft\windows\currentversion\explorer\
      Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus session info \setminus 0000000000000848d \setminus desktop \setminus names pace
      Opens key:
                                                                                          HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
```

08002b30309d}\shellfolder

Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder

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

08002b30309d}\shellfolder

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

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

08002b30309d}\shellfolder

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

Opens key:

a2ea-08002b30309d}

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

08002b30309d}\inprocserver32

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\apphelp.dll

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

Opens key: HKLM\software\microsoft\com3

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}

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

08002b30309d}\treatas

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

08002b30309d}\inprocserverx86

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

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

08002b30309d}\localserver32

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

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

08002b30309d}\inprochandler32

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

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

08002b30309d}\inprochandlerx86

Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86

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

08002b30309d}\localserver

Opens key:  $\label{eq:hkcr} \mbox{HKCR\clsid} \mbox{\sc 871c5380-42a0-1069-a2ea-08002b30309d} \mbox{\localserver} \mbox{\sc erver} \mbox{\sc$ 

Opens key:  $\qquad \qquad \text{HKLM} \\ \text{Software} \\ \text{microsoft} \\ \text{windows nt} \\ \text{currentversion} \\ \text{image file execution}$ 

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

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

Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}

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

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

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

 $000000000046 \} \ proxystubcl sid 32$ 

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

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

 $00c04f79abd1\\ \\ \ proxystubclsid32$ 

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

4ada335c892b}\shellfolder

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

Opens key:  $\label{local-bases-clsid-local-base$ 

00a0c91eedba}\shellfolder

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

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

0800361b1103}\shellfolder

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

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

00aa002f954e}\shellfolder

00a0c90dc849}\shellfolder

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

Opens key:

 $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} e$ 

```
HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-
  Opens key:
00c04fd91972}\inprocserver32
                                      HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972\}\inprocserver32
  Opens kev:
                                      HKLM\software\microsoft\windows\currentversion\app paths\cmd.exe
  Opens key:
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\policies\associations
  Opens key:
                                      HKCU \ software \ \verb|microsoft| windows \ \verb|currentversion| policies \ \verb|associations| \\
                                      HKCU\software\classes\.exe
  Opens key:
  Opens key:
                                      HKCR\.exe
                                      HKCU\software\classes\.ade
  Opens key:
                                      HKCR\.ade
  Opens key:
                                      HKCU\software\classes\.adp
  Opens key:
  Opens key:
                                      HKCR\.adp
  Opens key:
                                      HKCU\software\classes\.app
                                      HKCR\.app
  Opens key:
  Opens key:
                                      HKCU\software\classes\.asp
  Opens key:
                                      HKCR\.asp
                                      HKCU\software\classes\.bas
  Opens kev:
  Opens key:
                                      HKCR\.bas
  Opens key:
                                      HKCU\software\classes\.bat
  Opens key:
                                      HKCR\.bat
  Opens key:
                                      HKCU\software\classes\.cer
  Opens key:
                                      HKCR\.cer
                                      HKCU\software\classes\.chm
  Opens kev:
  Opens key:
                                      HKCR\.chm
  Opens key:
                                      HKCU\software\classes\.cmd
  Opens key:
                                      HKCR\.cmd
  Opens key:
                                      HKCU\software\classes\.com
  Opens key:
                                      HKCR\.com
  Opens key:
                                      HKCU\software\classes\.cpl
  Opens key:
                                      HKCR\.cpl
  Opens key:
                                      HKCU\software\classes\.crt
  Opens key:
                                      HKCR\.crt
  Opens key:
                                      HKCU\software\classes\.csh
  Opens key:
                                      HKCR\.csh
                                      HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens key:
  Opens key:
                                      HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens key:
                                      HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
  Opens key:
                                      HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
  Opens key:
                                      HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
  Opens key:
                                      HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
                                      HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
  Opens kev:
00c04fb6bfc4}\inprocserverx86
                                      HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86
  Opens kev:
  Opens key:
                                      HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\localserver32
  Opens key:
                                      HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32
                                      HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
  Opens kev:
00c04fb6bfc4}\inprochandler32
                                      HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
  Opens key:
                                      HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
  Opens key:
00c04fb6bfc4}\inprochandlerx86
                                      HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86
  Opens key:
  Opens kev:
                                      HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\localserver
                                      HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver
  Opens kev:
  Opens key:
                                      HKCU\software\microsoft\internet
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
                                      HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:
a2d8-08002b30309d}
  Opens key:
                                      HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
                                      Opens key:
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\setupapi.dll
  Opens key:
                                      HKLM\system\currentcontrolset\control\minint
  Opens key:
                                      HKLM\system\wpa\pnp
  Opens kev:
                                      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 key:
HKCU \setminus software \\ \mbox{$\currentversion} 
11e3-9fc7-806d6172696f}\
```

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

Opens key: HKCU\software\classes\directory

HKCR\directory Opens key:

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

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

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

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

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

Opens key: HKCR\directory\clsid

HKCU\software\classes\folder Opens key:

HKCR\folder Opens kev:

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

Opens key: HKCR\folder\clsid

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe

Opens key: HKCU\software\classes\exefile

HKCR\exefile Opens kev:

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

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

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

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

Opens key: HKCR\\*

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

HKCR\\*\clsid Opens key:

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

Opens key: HKCR\exefile\shell

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

Opens key: HKCR\exefile\shell\open

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

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

Opens key:

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

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

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

Opens key: HKCR\applications\cmd.exe

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

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

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

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\cmd.exe

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

b813f72dbb91}

Opens key:

7c29ddecae3f}

Opens key:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{94e3e076-8f53-42a5-8411-14414-1441-14414-144$ 085bcc18a68d}

Opens key:

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

Opens key:

```
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
 Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                            HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths
  Opens key:
  Opens key:
                            HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\shell} folders}
  Opens key:
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\cmd.exe
  Opens key:
                            HKLM\software\microsoft\windows
  Opens key:
                            HKLM\software\microsoft\windows\html help
                            HKLM\software\microsoft\windows\help
  Opens key:
  Opens key:
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acgenral.dll
 Opens key:
                            \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\shimeng.dll
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options\msacm32.dll
  Opens kev:
                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
  Opens key:
                            \label{lem:hklm} \verb+Kklm \+ software + microsoft + audiocompression manager + driver cache
  Opens key:
Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
                            HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
  Opens kev:
  Opens key:
Opens key:
                            HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
```

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1 Opens key: 

Opens key:

Opens key:

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

Opens key: 

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

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

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

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

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

Opens kev: 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

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

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\system\currentcontrolset\control\lsa

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

options\xpsp2res.dll

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

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

00aa004b2e24}\inprocserver32

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32

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

00aa004b2e24}\inprocserverx86

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

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

00aa004b2e24}\localserver32

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

Opens key:

00aa004b2e24}\inprochandler32

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

Opens key:

00aa004b2e24}\inprochandlerx86

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

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

00aa004b2e24}\localserver

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

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

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

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

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

Opens key:

HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32 HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-Opens kev:

00c04fb68820}\inprocserverx86

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

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

00c04fb68820}\localserver32

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver32 HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-Opens kev:

00c04fb68820}\inprochandler32

 $\label{lem:hkcr} $$ HKCR\clsid_{8bc3f05e-d86b-11d0-a075-00c04fb68820} \in $$ Abc3f05e-d86b-11d0-a075-00c04fb68820} $$ Abc3f05e-d86b-11d0-a075-00c04fb68820. $$ A$ Opens kev:

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

00c04fb68820}\inprochandlerx86

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

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

00c04fb68820}\localserver

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

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

Opens key:  $HKCU \setminus software \setminus classes \setminus interface \setminus \{f309ad18-d86a-11d0-a075-00c04fb68820\}$ 

HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820} Opens key: Opens key:  $HKCU \setminus software \setminus classes \setminus interface \setminus \{f309ad18 - d86a - 11d0 - a075 - d86a - 11d0 - a075 - d86a - d86a$ 

00c04fb68820}\proxystubclsid32 HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32 Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens key: Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24} Opens kev: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas  $HKCR\clsid$ {7c857801-7381-11cf-884d-00aa004b2e24}\treatas Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\inprocserver32 HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32 Opens key: Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86 Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86 HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-Opens key: 00aa004b2e24}\localserver32 HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32 Opens key: Opens kev: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32 Opens key:  $HKCR \ clsid \ \{7c857801-7381-11cf-884d-00aa004b2e24\} \ in prochandler 32$ Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandlerx86 HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandlerx86 Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-Opens kev: 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\software\classes\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887} Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887} Opens key: HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32 Opens key: Opens key:  $HKCU \setminus software \setminus classes \setminus interface \setminus \{9556dc99 - 828c - 11cf - a37e - 00aa003240c7\}$ Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7} HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-Opens key: 00aa003240c7}\proxystubclsid32 HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32 Opens kev: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} Opens key: Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\treatas HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens kev: ce99a996d9ea}\inprocserver32 HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32 Opens kev: Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\inprocserverx86 Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserverx86 HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens kev: ce99a996d9ea}\localserver32 HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver32 Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens key: ce99a996d9ea}\inprochandler32  $HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\tinprochandler 32$ Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-Opens kev: ce99a996d9ea}\inprochandlerx86 Opens key: Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504ce99a996d9ea}\localserver Opens key:  $HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver$ 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 key: HKLM\system\currentcontrolset\services\ldap Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdsapi.dll  $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key: options\fastprox.dll HKCU\software\classes\interface\{027947e1-d731-11ce-a357-000000000001} Opens kev: HKCR\interface\{027947e1-d731-11ce-a357-00000000001} Opens key: Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32  $\label{local-hkcr} \mbox{HKCR} $$ \mbox{Interface} \{027947e1-d731-11ce-a357-00000000001\} \proxystubclsid 32 \proxystubclsid 3$ Opens key: Opens key:  $HKCU \setminus software \setminus classes \setminus clsid \setminus \{1b1cad8c-2dab-11d2-b604-00104b703efd\}$ HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd} Opens kev: Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas

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

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

Opens key:

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\software\classes\interface\{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:  $\label{eq:hccn} \begin{tabular}{ll} HKCR\interface \{1c1c45ee-4395-11d2-b60b-00104b703efd\} \\ Opens key: \\ HKCU\software \classes \interface \{423ec01e-2e35-11d2-b604-00104b703efd\} \\ \end{tabular}$ 

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

00104b703efd}\proxystubclsid32

Queries value:

 $HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers [transparentenabled]|$ 

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[1bb90eca6f10f100c1d941d1fe06e7a9]

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

compatibility[1bb90eca6f10f100c1d941d1fe06e7a9]

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[rwlockresourcetimeout]

00000000046}[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableallforole32]

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]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]

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\currentcontrolset\control\nls\codepage[932]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]
Queries value: HKLM\system\currentcontrolset\services\disk\enum[0]

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

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\software\microsoft\windows\currentversion\internet

settings[disableimprovedzonecheck]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_protocol\_lockdown[1bb90eca6f10f100c1d941d1fe06e7a9.exe]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_protocol\_lockdown[\*]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-

ab78-1084642581fb]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-

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

Queries value:

settings[secureprotocols]

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

explorer\main[security\_hklm\_only]

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

settings[certificaterevocation]

```
Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[idnenabled]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[proxyhttp1.1]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:hkcu} in terms to the lemma of the lemm
settings[disablebasicoverclearchannel]
                                      HKCU\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
                                      HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[syncmode5]
                                      HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache[signature]
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings\5.0\cache\content[peruseritem]
                                      HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[peruseritem]
                                      HKLM\system\setup[systemsetupinprogress]
  Queries value:
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\content[cacheprefix]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\content[cachelimit]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\cookies[peruseritem]
                                      \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
  Queries value:
settings\5.0\cache\cookies[peruseritem]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\cookies[cachelimit]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
                                      \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
  Oueries value:
settings\5.0\cache\history[peruseritem]
                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[historv]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\history[cachelimit]
                                      HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                                      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]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
```

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

Queries value:

```
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
 Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\iecompat[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}.
 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]
                            \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\ietld[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                            \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\privacie:[cachepath]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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
 Oueries value:
settings[maxconnectionsperserver]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
 Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
                             HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperproxy]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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
 Oueries value:
settings[connectretries]
```

```
Oueries 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]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelifetime]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelimit]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[httpdefaultexpirytimesecs]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                            HKLM\software\microsoft\internet
 Queries value:
explorer \verb|\main| featurecontrol| feature_disable_unicode_handle_closing_callback[1bb90eca6f10f100c1d941d1fe06e7a9.exe]|
                            HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[perusercookies]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[leashlegacycookies]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypassftptimecheck]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablelegacypreauthasserver]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                            \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
 Queries value:
settings[bvpasssslnocachecheck]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
 Queries value:
                            \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[nocheckautodialoverride]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[dontusednsloadbalancing]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
 Queries value:
                            \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[sharecredswithwinhttp]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[mimeexclusionlistforcache]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[headerexclusionlistforcache]
 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[dnscacheenabled]
```

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

Queries value:

```
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]
                                                              \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
    Oueries value:
settings[warnonzonecrossing]
    Queries value:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertsending]
    Queries value:
                                                              \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings[warnonbadcertrecving]
    Oueries value:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
                                                              HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[alwaysdrainonredirect]
    Queries value:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
    Oueries 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]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
    Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (000000000003 \ [packed catalog item]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem]
    Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (0000000000006 [packed catalog item]) \ details \ 
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000008[packedcatalogitem]
    Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (000000000009[packed catalog item]) \ details \ de
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
    Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus namespace\_catalog \\ \setminus catalog\_entries \setminus 000000000001[library path]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
    Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ name space\_catalog \ na
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
    Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space \_ catalog 5 \ (catalog\_entries \ 000000000001 [supported name space]
    Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ set alog\_entries \ 000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
    Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
    Oueries value:
Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ name space\_catalog \ na
```

Oueries value:

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

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ (catalog\_entries \ 000000000003 \ [displaystring]$ Oueries value:

Oueries value:

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

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000003 [supported name space]]$ Oueries value:

Queries value:

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

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

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]

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

settings[enableautodial]

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

settings[urlencoding]

Queries value: Queries value:

Oueries value:

Queries value:

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

settings[truncatefilename]

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

settings[badproxyexpirestime]

HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Oueries 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] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midil Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Queries value: Oueries value:  $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi4]$  $HKLM \backslash software \backslash microsoft \backslash windows \ nt \backslash current version \backslash drivers 32 [midi5]$ Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi91 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2] Queries 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] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]

HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2] Oueries value:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ drivers 32 [mixer 3]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] Oueries 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9] Queries value:

HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries] Queries value:

HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout] HKLM\software\microsoft\tracing[enableconsoletracing] Oueries value: Oueries value: HKLM\software\microsoft\tracing\rasapi32[enablefiletracing] Queries value: HKLM\software\microsoft\tracing\rasapi32[filetracingmask] Oueries value: HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing] Queries value: HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]

Queries value: HKLM\software\microsoft\tracing\rasapi32[maxfilesize] Queries value: HKLM\software\microsoft\tracing\rasapi32[filedirectory]

Queries 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]

Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[personal]

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

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]

Queries value: HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]

Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Queries 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]
Queries value: HKCU\software\microsoft\windows

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]

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

settings[proxyenable]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

settings\connections[savedlegacysettings]

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

settings\connections[defaultconnectionsettings]

Queries value: HKLM\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature\_mime\_handling[1bb90eca6f10f100c1d941d1fe06e7a9.exe]|$ 

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_mime\_handling[\*]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdl1]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]

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

explorer\security[disablesecuritysettingscheck]

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

settings\zones\0[flags]

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

settings\zones\1[flags]

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

settings\zones\2[flags]

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

settings\zones\3[flags]

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

settings\zones\4[flags]

Oueries value: HKCU\software\microsoft\internet

 $explorer \verb|\main| featurecontrol \verb|\feature| local machine_lock down[1bb90eca6f10f100c1d941d1fe06e7a9.exe]| local machine_lock down[1bb90eca6f10f100c1d941d$ 

Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_localmachine\_lockdown[\*] Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature\_localmachine\_lockdown[1bb90eca6f10f100c1d941d1fe06e7a9.exe]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_localmachine\_lockdown[\*]

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

settings[createuricachesize]

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

settings[createuricachesize]

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

settings[enablepunycode]

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

settings[enablepunycode]

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

settings\zonemap[autodetect]

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

settings\zones\3[1a10]

Oueries value:  $HKLM \verb|\system| current controlset \verb|\services| dnscache \verb|\parameters[queryadaptername]|$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Oueries value: 

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

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Oueries value:  $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[enabledhcp] Oueries value: c7d49d7cecdc}[leaseobtainedtime] Oueries value:  $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[leaseterminatestime] Queries value: c7d49d7cecdc}[dhcpserver] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: HKLM\software\microsoft\rpc\securityservice[10] Queries value:  $HKLM \verb|\system| current controls et \verb|\control| security providers [security providers]|$ Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment] HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities] HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid] Queries 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:  $HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus msapsspc.dll[tokensize]$ HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name] Queries value: Oueries value: c7d49d7cecdc}[queryadaptername] Queries value: c7d49d7cecdc}[disableadapterdomainname] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registrationenabled] Queries value: c7d49d7cecdc}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registrationmaxaddresscount] Oueries value:  $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4300-abe3-4300-a$ c7d49d7cecdc}[maxnumberofaddressestoregister] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[domain] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid] Oueries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version] Queries value: c7d49d7cecdc}[dhcpdomain] HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize] Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name] Oueries value: Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities] HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid] Oueries 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]

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[ipautoconfigurationenabled]

Queries value:

c7d49d7cecdc}[addresstype]

Oueries value: c7d49d7cecdc}[nameserver] c7d49d7cecdc}[dhcpnameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder] Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type] Queries value:  $HKLM \ software \ microsoft \ strong$ cryptographic provider[image path] HKLM\software\microsoft\cryptography[machineguid] Oueries value: Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel] Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Queries 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] HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps] Queries value: Queries value: HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood] HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Queries value:  $HKCU \ software \ microsoft \ windows \ current version \ policies \ \ explorer [no common groups]$  $HKLM \ software \ microsoft \ windows \ current version \ explorer \ desktop \ names pace \ \{11016101-e366-4d22-e4d22-e4d24$ bc06-4ada335c892b}[suppressionpolicy] ba4f-00a0c91eedba}[suppressionpolicy] HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{450d8fba-ad25-11d0-98a8-0800361b1103}[suppressionpolicy] 9f08-00aa002f954e}[suppressionpolicy] HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{e17d4fc0-5564-11d1-83f2-00a0c90dc849}[suppressionpolicy] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[wantsparsedisplayname] Queries value: HKCR\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[wantsparsedisplayname] HKCR\clsid\{871c5380-42a0-1069-a2ea-Oueries value: 08002b30309d}\shellfolder[wantsparsedisplayname] HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[] Queries value: Oueries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[loadwithoutcom] HKLM\software\microsoft\windows\currentversion\shell extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}] Oueries value: 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}} 0x4011 HKCU\software\microsoft\windows\currentversion\shell extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}} 0x4011 HKLM\system\currentcontrolset\control\session Oueries value: manager\appcompatibility[disableappcompat] Queries value: HKLM\software\microsoft\com3[com+enabled] Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess] HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject] Oueries value: Queries value: HKLM\software\microsoft\com3[regdbversion] HKCR\clsid\{871c5380-42a0-1069-a2ea-Oueries value:

08002b30309d}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]

HKCR\clsid\{871c5380-42a0-1069-a2ea-

HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]

08002b30309d}\inprocserver32[inprocserver32]

Queries value: Queries value:

```
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[]
  Queries value:
                                    HKLM\software\microsoft\internet explorer\setup[installstarted]
  Oueries value:
  Queries value:
                                    HKCR \land ext{b722bccb-4e68-101b-a2bc-00aa00404770} \land proxystubclsid32[]
  Oueries value:
                                    HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
                                    HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[]
  Oueries value:
  Oueries value:
                                    HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32[]
  Oueries value:
                                    HKCR\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[wantsparsedisplayname]
  Queries value:
                                    HKCR\clsid\{1f4de370-d627-11d1-ba4f-
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]
  Queries value:
                                    HKCR\clsid\{e17d4fc0-5564-11d1-83f2-
00a0c90dc849}\shellfolder[wantsparsedisplayname]
                                    HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
  Oueries value:
  Queries value:
                                    HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
00c04fd91972}\inprocserver32[loadwithoutcom]
                                    HKCR\.exe[]
  Oueries value:
  Queries value:
                                    HKCR\.asp[]
  Queries value:
                                    HKCR\.bat[]
                                    HKCR\.cer[]
  Queries value:
  Queries value:
                                    HKCR\.chm[]
  Queries value:
                                    HKCR\.cmd[]
                                    HKCR\.com[]
  Oueries value:
                                    HKCR\.cpl[]
  Queries value:
                                    HKCR\.crt[]
  Oueries value:
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
  Queries value:
00c04fb6bfc4}\inprocserver32[inprocserver32]
  Queries value:
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
  Oueries value:
                                    HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
  Queries value:
00c04fb6bfc4}\inprocserver32[threadingmodel]
  Oueries 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]
  Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [noset folders]
                                    Queries value:
                                    HKLM\svstem\wpa\pnp[seed]
  Oueries value:
  Queries value:
                                    HKLM\system\setup[osloaderpath]
  Oueries value:
                                    HKLM\system\setup[systempartition]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion[devicepath]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\setup[loglevel]
                                    HKLM\software\microsoft\windows\currentversion\setup[logpath]
  Queries value:
  Queries value:
11e3-9fc7-806d6172696f}[data]
  Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints \ 2 \ cpc \ volume \ \{f90255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-6bc4-f80255c2-
11e3-9fc7-806d6172696f}[generation]
                                    HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
  Queries value:
409d6c4515e9}[drivemask]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
  Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ policies \ explorer [nonet crawling]
```

Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenul Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Queries 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] Oueries 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] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling] HKCR\directory[docobject] Queries value: HKCR\directory[browseinplace] Queries value: Queries value: HKCR\directory[isshortcut] Queries value: HKCR\directory[alwaysshowext] Oueries value: HKCR\directory[nevershowext] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions] Queries value: HKCR\exefile[docobject] HKCR\exefile[browseinplace] Queries value: Queries value: HKCR\exefile[isshortcut] Oueries value: HKCR\exefile[alwaysshowext] HKCR\exefile[nevershowext] Queries value: HKCR\exefile\shell[] Oueries value: Oueries value: HKCR\exefile\shell\open\command[] HKCR\exefile\shell\open\command[command] Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Queries value: 1757981266-507921405-1957994488-1003[flags] HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Queries value: 1757981266-507921405-1957994488-1003[state]  $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and the current version \$ Queries value: 1757981266-507921405-1957994488-1003[userpreference] HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Queries 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:  $HKCU \ software \ microsoft \ windows \ shell no roam \ muicache \ [c:\windows \ system 32 \ cmd.exe]$ Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun] Queries value: Queries value: HKLM\system\wpa\mediacenter[installed] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]  $\label{lem:hklmsoftware policies microsoft windows safer code identifiers [levels] \\$ Queries value: be2efd2c1a33}[itemdata] Oueries value: be2efd2c1a33}[saferflags] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[itemdata] Oueries value:

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

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

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

edd5fbde1328}[hashalg]
Oueries value:

edd5fbde1328}[itemsize]

edd5fbde1328}[saferflags]
Oueries value:

Queries value:

Oueries value:

Oueries value:

Oueries value:

Queries value:

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemsize]

Oueries value:

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-085bcc18a68d\} [item \ data]$ 

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[hashalg]

Queries value:

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[saferflags]

Queries value:

 $HKLM \ software \ b01icies \ icrosoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} \ [itemdata]$ 

Queries value:

Queries value:

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

Queries value:

 $HKLM \ software \ b01icies \ icrosoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} \ [saferflags]$ 

Queries value:

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

Oueries 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]

Oueries value:

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

Queries value

 $\label{localization} HKLM \software \mbox{$m$icrosoft$-audiocompression manager$} \label{localization} HKLM \software \mbox{$m$icrosoft$-audiocompression manager$} \label{localization}$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\mbox{\sc manager} \arrows of the discompression manager \driver cache \mbox{\sc manager} adpcm [aformattag cache] Queries value:$ 

HKLM\software\microsoft\audiocompressionmanager\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]
 Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
 Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
Queries value:

 $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msadpcm \ [cfilter tags]$ 

Queries value: HKLM\software\microsoft\windows

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:  $HKLM \ \ software \ \ microsoft \ \ \ audio compression manager \ \ \ \ \ \ msg711 [a formattag cache]$ Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags] HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msgsm610] Oueries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags] Oueries value: 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:  $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} which is a constant, and in the lemma substitution of the l$ Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags] HKLM\software\microsoft\windows Oueries value: 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\software\microsoft\windows nt\currentversion\drivers32[msacm.msaudio1] Oueries value: Oueries value:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msaudio1 [cformattags]$ HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache] Oueries value:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msaudio1[cfilter tags]$ Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.sl\_anet] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[fdwsupport] Queries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[aformattagcache] Oueries value:  $HKLM \verb|\software\microsoft\audiocompression| manager \verb|\drivercache\msacm.sl_anet[cfiltertags]| \\$ Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport] Oueries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags] Oueries value:  $\label{local-operator} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\drivers 32[msacm.13acm]} \mbox{\sc microsoft\windows} \mbox{\sc micro$ 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] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags] Queries value: HKCU\software\microsoft\multimedia\audio compression manager\msacm[nopcmconverter] HKCU\software\microsoft\multimedia\audio compression manager\priority Oueries value:

Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]
Queries value: HKLM\software\microsoft\command processor[disableunccheck]

v4.00[priority1]

```
Oueries value:
                          HKLM\software\microsoft\command processor[enableextensions]
 Oueries value:
                          HKLM\software\microsoft\command processor[delayedexpansion]
 Oueries value:
                          HKLM\software\microsoft\command processor[defaultcolor]
                          HKLM\software\microsoft\command processor[completionchar]
 Queries value:
 Oueries value:
                          {\tt HKLM \setminus software \setminus microsoft \setminus command processor[pathcompletion char]}
 Queries value:
                          HKLM\software\microsoft\command processor[autorun]
 Oueries value:
                          HKCU\software\microsoft\command processor[disableunccheck]
 Oueries value:
                          HKCU\software\microsoft\command processor[enableextensions]
 Oueries value:
                          HKCU\software\microsoft\command processor[delayedexpansion]
 Oueries value:
                          HKCU\software\microsoft\command processor[defaultcolor]
                          HKCU\software\microsoft\command processor[completionchar]
 Oueries value:
 Queries value:
                          HKCU\software\microsoft\command processor[pathcompletionchar]
 Oueries value:
                          HKCU\software\microsoft\command processor[autorun]
                          Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\compatibility32[tasklist]
 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]
 Oueries value:
                          HKLM\software\microsoft\ole[maximumallowedallocationsize]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
 Queries value:
                         HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
 Queries value:
                         HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
 Queries value:
                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]
                         HKCR\clsid\{4590f811-1d3a-11d0-891f-
 Oueries value:
00aa004b2e24}\inprocserver32[threadingmodel]
 Queries value:
                         HKLM\software\microsoft\wbem\cimom[repository directory]
                          HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
 Queries value:
 Queries value:
                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[dllsurrogate]
 Queries value:
                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
                          HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32[]
 Oueries value:
                         HKCR\clsid\{7c857801-7381-11cf-884d-
 Queries value:
00aa004b2e24}\inprocserver32[inprocserver32]
                         HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
 Oueries value:
 Queries value:
                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
 Queries value:
                         HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
                          HKCR \ interface \ \{d4781cd6-e5d3-44df-ad94-930efe48a887\} \ proxystubclsid32[]
 Queries value:
                          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[]
 Queries value:
                         HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
 Oueries value:
 Queries value:
                         HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[threadingmodel]
                         HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[processid]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[contextlimit]
                          HKLM\software\microsoft\wbem\cimom[objectlimit]
 Queries value:
                          HKLM\software\microsoft\wbem\cimom[identifierlimit]
 Oueries value:
 Queries value:
                          HKCR \ interface \ \{027947e1-d731-11ce-a357-00000000001\} \ proxystubclsid \ 32[]
                         HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
 Oueries value:
00104b703efd}\inprocserver32[inprocserver32]
                         HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
 Oueries value:
 Queries value:
                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[appid]
 Queries value:
                         HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
                          HKCR \ interface \ \{1c1c45ee-4395-11d2-b60b-00104b703efd\} \ proxystubclsid32[]
 Queries value:
                          HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]
 Oueries value:
 Value changes:
                          HKLM\software\microsoft\cryptography\rng[seed]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
 Value changes:
                          \label{local-constraint} \mbox{HKCU\software\mbox{\sc urrentversion\explorer\shell}} \mbox{}
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]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
                          HKCU\software\microsoft\windows\currentversion\internet
 Value changes:
settings\zonemap[intranetname]
```

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]

Value changes:

806d6172696f}[baseclass]