Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 4, Task ID: 14

Task ID: 14 Risk Level: 6

Date Processed: 2016-03-29 03:27:45 (UTC)

Processing Time: 61.54 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\test12.jar.exe"

Sample ID: 4
Type: basic
Owner: admin
Label: test12.jar

Date Added: 2016-03-29 03:27:44 (UTC)
File Type: archive:jar:applet
File Size: 6213 bytes

MD5: 0fa3c06281d3b260bfccbb5a22dd74c5

SHA256: 1b7e0322a81be961ebce33aaeb395124544cfb01a3ab54f23cf64400fb2b04c7

Description: None

Pattern Matching Results

6 Writes to system32 folder

2 ZIP archive format

3 Long sleep detected

Process/Thread Events

Creates process: C:\Program Files\Internet Explorer\iexplore.exe ["C:\Program

Files\Internet Explorer\iexplore.exe" "c:\windows\temp\test12.jar.html"]

Creates process: C:\Program Files\Internet Explorer\iexplore.exe ["C:\Program

Files\Internet Explorer\iexplore.exe" SCODEF:652 CREDAT:79873]

Creates process: C:\Program Files\Java\jre7\bin\java.exe ["C:\Program

Files\Java\jre7\bin\java.exe" -D_jvm_launched=11225877405 -D_applet_launched=11225800879 -

 $X bootclass path/a: C: \PROGRA-1 \Java \jre7 \lib \jevaws.jar; C: \PROGRA-1 \Java \Java$

 $-Djava.class.path=C:\PROGRA~1\Java\jre7\classes \ -Dsun.awt.warmup=true$

sun.plugin2.main.client.PluginMain

write_pipe_name=jpi2_pid1628_pipe3,read_pipe_name=jpi2_pid1628_pipe2]

Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]

Named Object Events

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\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

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

1957994488-1003

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

1957994488-1003

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

1957994488-1003

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

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003 Creates mutex: \BaseNamedObjects\!BrowserEmulation!SharedMemory!Mutex

Creates mutex: \BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex: \BaseNamedObjects\ConnHashTable<652>_HashTable_Mutex

Creates mutex: \BaseNamedObjects\oleacc-msaa-loaded
Creates mutex: \BaseNamedObjects\ZonesCounterMutex

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

Creates mutex: \BaseNamedObjects_!SHMSFTHISTORY!_

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

settings!history!history.ie5!mshist012016032920160330!

Creates mutex: \BaseNamedObjects\DDrawWindowListMutex
Creates mutex: \BaseNamedObjects_DDrawExclMode__
Creates mutex: \BaseNamedObjects_DDrawCheckExclMode__
Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.EIH

Creates event: \BaseNamedObjects\Isolation Signal Registry Event (3AF75141-F55E-11E5-

AE32-08002719344D, 0)

Creates event: \BaseNamedObjects\IE_EarlyTabStart_Oxfc

Creates event: \BaseNamedObjects\Isolation Signal Registry Event (3AF75142-F55E-11E5-

AE32-08002719344D, 0)

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

Creates event: \BaseNamedObjects\IEFrame.EventCheckDefaultBrowser

\BaseNamedObjects\jpi2_pid1628_evt1 Creates event:

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

\BaseNamedObjects\IEFrame!GetAsyncKeyStateQuery!652 Creates semaphore: Creates semaphore: \BaseNamedObjects\IEFrame!GetAsyncKeyStateReply!652

Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57} Creates semaphore: \BaseNamedObjects\shell.{090851A5-EB96-11D2-8BE4-00C04FA31A66}

Creates semaphore: \BaseNamedObjects\OleDfRoot000023217 Creates semaphore: \BaseNamedObjects\OleDfRoot0000235CA

File System Events

C:\Documents and Settings\Admin\Local Settings\Application

Data\Microsoft\Internet Explorer\Recovery\Active\RecoveryStore.{3AF75143-F55E-11E5-AE32-

08002719344D}.dat

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\~DF321B.tmp Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Microsoft\Internet Explorer\Recovery\Active\{3AF75145-F55E-11E5-AE32-08002719344D}.dat C:\Documents and Settings\Admin\Local Settings\Temp\~DF35CE.tmp Creates:

C:\DOCUME~1\Admin\LOCALS~1\Temp\hsperfdata_Admin Creates:

Creates: C:\Documents and Settings\Admin\Local

Settings\Temp\hsperfdata_Admin\1628

C:\Documents and Settings\Admin\Local Creates:

Settings\History\History.IE5\MSHist012016032920160330

C:\Documents and Settings\Admin\Local Creates: $Settings \verb|\History\EE5\MSHist012016032920160330\index.dat$ C:\Documents and Settings\Admin\Local Creates

Settings\Temp\hsperfdata_Admin\1252

C:\WINDOWS\system32\d3d9caps.tmp Creates:

Creates C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\0

Creates: C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\1

Creates: C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\2 C:\Documents and Settings\Admin\Local Settings\Application

Creates

Data\Sun\Java\Deployment\cache\6.0\3 Creates: ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}$

Data\Sun\Java\Deployment\cache\6.0\4

Creates: C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\5

Creates C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\6

Creates: C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\7

C:\Documents and Settings\Admin\Local Settings\Application Creates:

Data\Sun\Java\Deployment\cache\6.0\8

Creates C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\9 Creates:

C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\10

C:\Documents and Settings\Admin\Local Settings\Application Creates: Data\Sun\Java\Deployment\cache\6.0\11

Creates C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\12

Creates

C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\13

C:\Documents and Settings\Admin\Local Settings\Application Creates:

 $Data \S un \S ava \S eployment \S ache \S 6.0 \S 14$

 ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}$ Data\Sun\Java\Deployment\cache\6.0\15

Creates C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\16

C:\Documents and Settings\Admin\Local Settings\Application Creates:

Data\Sun\Java\Deployment\cache\6.0\17

 ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}$ Creates: Data\Sun\Java\Deployment\cache\6.0\18

Creates C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\19

Creates: C:\Documents and Settings\Admin\Local Settings\Application

Data\Sun\Java\Deployment\cache\6.0\20

C:\Documents and Settings\Admin\Local Settings\Application Creates:

Data\Sun\Java\Deployment\cache\6.0\21

Creates

 ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}$ Data\Sun\Java\Deployment\cache\6.0\22

Creates:

C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java\Deployment\cache\6.0\23

C:\Documents and Settings\Admin\Local Settings\Application Creates: Data\Sun\Java\Deployment\cache\6.0\24

Creates: ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}$

Data\Sun\Java\Deployment\cache\6.0\25

Creates: C:\Documents and Settings\Admin\Local Settings\Application

Data (Car) Israel Dari Israel)			
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment	\cache\6.0\27		•	
Creates: Data\Sun\Java\Deployment		and	Settings\Admin\Local	Settings\Application
Creates:	C:\Documents	and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment	\cache\6.0\30		•	
<pre>Creates: Data\Sun\Java\Deployment</pre>		and	Settings\Admin\Local	Settings\Application
Creates:	C:\Documents	and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Settings\Annlication
Data\Sun\Java\Deployment	\cache\6.0\33		•	
Creates: Data\Sun\Java\Deployment		and	Settings\Admin\Local	Settings\Application
Creates:		and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Sottings\Application
Data\Sun\Java\Deployment		anu	Sectings (AdmitiveCotal	Sectings (Application
Creates: Data\Sun\Java\Deployment		and	Settings\Admin\Local	Settings\Application
Creates:		and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Sattings\Application
Data\Sun\Java\Deployment		anu	Sectings (AdmitiveOcal	Sectings (Application
<pre>Creates: Data\Sun\Java\Deployment</pre>		and	Settings\Admin\Local	Settings\Application
Creates:	C:\Documents	and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Settings\Annlication
Data\Sun\Java\Deployment	\cache\6.0\42		•	
Creates: Data\Sun\Java\Deployment		and	Settings\Admin\Local	Settings\Application
Creates:	C:\Documents	and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment			C-++:\	C-++:\
<pre>Creates: Data\Sun\Java\Deployment</pre>		anu	Settings\Admin\Local	Sectings (Application
<pre>Creates: Data\Sun\Java\Deployment</pre>		and	Settings\Admin\Local	Settings\Application
Creates:	C:\Documents	and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment		and	Cottings \ Admin \ Local	Settings\Application
<pre>Creates: Data\Sun\Java\Deployment</pre>		anu	Sectings (AdmitiveOcal	Sectings (Application
Creates: Data\Sun\Java\Deployment		and	Settings\Admin\Local	Settings\Application
Creates:	C:\Documents	and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Settings\Annlication
Data\Sun\Java\Deployment	\cache\6.0\53		· ·	0 11
Creates: Data\Sun\Java\Deployment		and	Settings\Admin\Local	Settings\Application
Creates:	C:\Documents	and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment	\cache\6.0\56		-	
Creates: Data\Sun\Java\Deployment		and	Settings\Admin\Local	Settings\Application
Creates:		and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Cottings\Application
Data\Sun\Java\Deployment	\cache\6.0\60		•	
<pre>Creates: Data\Sun\Java\Deployment</pre>		and	Settings\Admin\Local	Settings\Application
Creates:	C:\Documents	and	Settings\Admin\Local	Settings\Application
<pre>Data\Sun\Java\Deployment Creates:</pre>		and	Settings\Admin\Local	Settings\Application
Data\Sun\Java\Deployment	\cache\6.0\63		•	
Opens: Opens:	C:\WINDOWS\Pi	refet	tch\IEXPLORE.EXE-27122	2324.pt
Opens:	C:\		Cattein	
Opens: Opens:	<pre>C:\Documents C:\Documents</pre>		Settings Settings\Admin	
Opens:			Settings\Admin\Cookie	es
Opens:			Settings\Admin\Local	
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 Files
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\QXMNQBKF
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X
 Opens:
                         C:\Program Files
                         C:\Program Files\Internet Explorer
 Opens:
 Opens:
                         C:\WINDOWS
 Opens:
                         C:\WINDOWS\Registration
 Opens:
                         C:\WINDOWS\system32
                         C:\WINDOWS\system32\en-US
 Opens:
 Opens:
                         C:\WINDOWS\WinSxS
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
 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
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe
 Opens:
                         C:\WINDOWS\system32\advapi32.dll
 Opens:
                         C:\WINDOWS\system32\rpcrt4.dll
 Opens:
                         C:\WINDOWS\system32\secur32.dll
 Opens:
                         C:\WINDOWS\system32\user32.dll
 Opens:
                         C:\WINDOWS\system32\gdi32.dll
                         C:\WINDOWS\system32\msvcrt.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\shlwapi.dll
 Opens:
                         C:\WINDOWS\system32\shell32.dll
 Opens:
                         C:\WINDOWS\system32\ole32.dll
 Opens:
                         C:\WINDOWS\system32\iertutil.dll
 Opens:
                         C:\WINDOWS\system32\urlmon.dll
 Opens:
                         C:\WINDOWS\system32\oleaut32.dll
 Opens:
                         C:\WINDOWS\system32\imm32.dll
 Opens:
                         C:\WINDOWS\system32\ctype.nls
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\sortkey.nls
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
 Opens:
                         C:\WINDOWS\system32\comdlg32.dll
 Opens:
                         C:\WINDOWS\system32\rpcss.dll
 Opens:
                         C:\WINDOWS\system32\MSCTF.dll
 Opens:
                         C:\Program Files\Internet Explorer\sqmapi.dll
                         C:\WINDOWS\system32\winlogon.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
                         C:\WINDOWS\system32\xpsp2res.dll
 Opens:
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\WINDOWS\system32\version.dll
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
                         C:\Program Files\Internet Explorer\ieproxy.dll
 Opens:
                         C:\WINDOWS\system32\wininet.dll
                         C:\WINDOWS\system32\normaliz.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\mlang.dll
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
                         {\tt C:\WINDOWS\system32\MSCTFIME.IME}
 Opens:
 Opens:
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
                         C:\WINDOWS\system32\sxs.dll
                         {\tt C:\WINDOWS\system32\actxprxy.dll}\\
 Opens:
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
                         C:\WINDOWS\system32\rasman.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\tapi32.dll
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\winmm.dll
 Opens:
                         C:\WINDOWS\system32\userenv.dll
 Opens:
                         C:\WINDOWS\system32\sensapi.dll
 Opens:
                         C:\WINDOWS\system32\msv1_0.dll
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
                         C:\WINDOWS\system32\narrhook.dll
 Opens:
```

C:\WINDOWS\system32\oleacc.dll

Opens:

```
C:\WINDOWS\system32\msvcp60.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\oleaccrc.dll
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
 Opens:
                         C:\WINDOWS\system32\stdole2.tlb
 Opens:
                         C:\WINDOWS\system32\msimg32.dll
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\urlmon.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\IEFRAME.dll.123.Manifest
                         C:\WINDOWS\system32\IEFRAME.dll.123.Config
 Opens:
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\Desktop
 Opens:
                         C:\Program Files\Common Files
 Opens:
                         C:\Program Files\Common Files\Adobe
 Opens:
                         C:\Program Files\Common Files\Adobe\Acrobat
 Opens:
                         C:\Program Files\Java
 Opens:
                         C:\Program Files\Java\jre7
 Opens:
                         C:\Program Files\Java\jre7\bin
 Opens:
                         C:\WINDOWS\Temp
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe.Manifest
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                         C:\AUTOEXEC.BAT
 Opens:
                         {\tt C:\Documents\ and\ Settings\All\ Users\Application}
Data\Microsoft\Network\Connections\Pbk
 Opens:
                         C:\WINDOWS\system32\ras
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\Network\Connections\Pbk\
 Opens:
                         C:\WINDOWS\system32\ieui.dll
                         C:\Program Files\Internet Explorer\xpshims.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\cscui.dll
 Opens:
                         C:\WINDOWS\system32\cscdll.dll
                         C:\WINDOWS\System32\cscui.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\System32\cscui.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\url.dll
 Opens:
                         C:\Documents and Settings\Admin\Favorites\Desktop.ini
 Opens:
                         C:\WINDOWS\system32\xmllite.dll
 Opens:
                         C:\WINDOWS\system32\xpsp3res.dll
                         C:\Program Files\Messenger\msmsgs.exe
 Opens:
 Opens:
                         C:\WINDOWS\Fonts\SEGOEUI.TTF
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Manifest
                         C:\WINDOWS\system32\MLANG.dll.123.Config
 Opens:
 Opens:
                         C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
                         C:\Program Files\Common
 Opens:
Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll.2.Manifest
                         C:\Program Files\Common
Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll.2.Config
 Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca
 Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcr80.dll
 Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcp80.dll
 Opens:
                         C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
 Opens:
                         C:\Program Files\Common
Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll.2.Manifest
 Opens:
                         C:\Program Files\Common
Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll.2.Config
 Opens:
                         C:\Program Files\Java\jre7\bin\jp2ssv.dll
 Opens:
                         C:\Program Files\Java\jre7\bin\msvcr100.dll
 Opens:
                         C:\WINDOWS\system32\en-US\urlmon.dll.mui
 Opens:
                         C:\WINDOWS\Temp\test12.jar.html
 Opens:
                         C:\WINDOWS\system32\mshtml.dll
 Opens:
                         C:\WINDOWS\system32\msls31.dll
 Opens:
                         C:\WINDOWS\system32\psapi.dll
                         C:\Program Files\Java\jre7\bin\jp2iexp.dll
 Opens:
 Opens:
                         C:\Program Files\Java\jre7\bin\client
 Opens:
                         C:\Program Files\Java\jre7\bin\client\jvm.dll
                         C:\PROGRA~1\Java\jre7\bin\client\jvm.dll.2.Manifest
 Opens:
                         C: \PROGRA~1\Java\jre7\bin\client\jvm.dll.2.Config
 Opens:
 Opens:
                         C:\WINDOWS\system32\wsock32.dll
 Opens:
                         C:\Program Files\Java\jre7\bin\verify.dll
 Opens:
                         C:\Program Files\Java\jre7\bin\java.dll
 Opens:
                         C:.hotspotrc
                         C:\Documents and Settings\Admin\Local Settings\Temp\hsperfdata_Admin
 Opens:
 Opens:
                         C:\Program Files\Java\jre7\bin\zip.dll
```

```
C:\WINDOWS\Fonts\times.ttf
 Opens:
 Opens:
                         C:\Program Files\Java\jre7\lib
                         C:\Program Files\Java\jre7\lib\meta-index
 Opens:
 Opens:
                         C:\Program Files\Java\jre7\bin\client\classes.jsa
 Opens:
                         C:\WINDOWS\system32\en-US\mshtml.dll.mui
 Opens:
                         C:\Program Files\Java\jre7\lib\rt.jar
                         C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012014033120140407
                         C:\Documents and Settings\Admin\Local
Settings \verb|\History\History\E5| MSH is to 12014033120140407 \verb|\index.dat| 
 Opens:
                         C:\WINDOWS\Temp\404ddfd0-b2d3-4483-abb5-cc3aec4357f3
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413\index.dat
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\History\History.IE5\MSHist012016032920160330
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings \verb|\History.IE5| MSH is to 12016032920160330 \verb|\Index.dat| \\
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\frameiconcache.dat
                         C:\Program Files\Java\jre7\lib\deploy.jar
 Opens:
 Opens:
                         C:\Program Files\Java\jre7\lib\javaws.jar
 Opens:
                         C:\Program Files\Java\jre7\lib\plugin.jar
 Opens:
                         C:.hotspot_compiler
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
                         C:\Program Files\Java\jre7\lib\ext\meta-index
 Opens:
 Opens:
                         C:\WINDOWS\system32\msasn1.dll
 Opens:
                         C:\Program Files\Java\jre7\lib\ext
 Opens:
                         C:\Program Files\Java\jre7\bin\deploy.dll
 Opens:
                         C:\Program Files\Java\jre7\bin\jp2native.dll
 Opens:
                         C:\WINDOWS\system32\netmsg.dll
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\deployment.properties
 Opens:
                         C:\Program Files\Java\jre7\bin\net.dll
 Opens:
                         C:\Program Files\Java\jre7\bin\nio.dll
 Opens:
                         C:\Program Files\Java\jre7\lib\security\java.security
 Opens:
                         C:\Program Files\Java\jre7\bin\java.exe
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
                         C:\Program Files\Java\jre7\bin\java.exe.Manifest
                         C:\Program Files\Java\jre7\bin\java.exe.Config
 Opens:
 Opens:
                         C:\WINDOWS\Prefetch\JAVA.EXE-1E21D4DA.pf
 Opens:
                         C:\Documents and Settings\Admin\Application Data
                         {\tt C:\Documents\ and\ Settings\Admin\Application\ Data\Sun}
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Application Data\Sun\Java
                         C:\Documents and Settings\Admin\Application Data\Sun\Java\Deployment
 Opens:
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\cache
                         C:\Documents and Settings\Admin\Local Settings\Application Data
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application Data\Sun
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application Data\Sun\Java
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Sun\Java\Deployment
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
.
Data\Sun\Java\Deployment\cache
                         C:\Documents and Settings\Admin\Local Settings\Temp
 Opens:
 Opens:
                         C:\Program Files\Java\jre7\lib\i386
 Opens:
                         C:\Program Files\Java\jre7\lib\security
 Opens:
                         C:\System Volume Information
 Opens:
                         C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}
                         C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
 Opens:
0D4648AC633B}\RP24
 Opens:
                         C:\WINDOWS\AppPatch
                         C:\WINDOWS\system32\shimeng.dll
 Opens:
 Opens:
                         C:\Program Files\Java\jre7\lib\i386\jvm.cfg
 Opens:
                         C:\Program Files\Java\jre7\bin\awt.dll
                         C:\DOCUME~1\ADMIN\LOCALS~1\TEMP\HSPERFDATA_ADMIN\2912
 Opens:
 Opens:
                         C:\WINDOWS\system32\d3d9.dll
 Opens:
                         C:\WINDOWS\system32\d3d8thk.dll
 Opens:
                         C:\WINDOWS\system32\vga.dll
 Opens:
                         C:\WINDOWS\system32\d3d9caps.dat
                         C:\WINDOWS\SYSTEM32\D3D9CAPS.TMP
 Opens:
 Opens:
                         C:\WINDOWS\system32\vga256.dll
 Opens:
                         C:\WINDOWS\system32\vga64k.dll
                         C:\Program Files\Java\jre7\lib\net.properties
 Opens:
                         C:\SYSTEM VOLUME INFORMATION\_RESTORE{DFC4753E-A69F-4404-9702-
 Opens:
OD4648AC633B}\RP24\CHANGE.LOG
                         C:\Program Files\Java\jre7\lib\security\java.policy
 Opens:
 Opens:
                         C:\Program Files\Java\jre7\bin\client\jvm.dll.2.Manifest
```

```
C:\Program Files\Java\jre7\bin\client\jvm.dll.2.Config
 Opens:
                          C:\WINDOWS\system32\d3d9caps.tmp
 Opens:
                          C:\Documents and Settings\Admin\.accessibility.properties
 Opens:
 Opens:
                          C:\Program Files\Java\jre7\lib\accessibility.properties
 Opens:
                          C:\WINDOWS\Sun
 Opens:
                          C:\WINDOWS\Sun\Java
                          C:\Documents and Settings\Admin\.java.policy
 Opens:
                          C:\Documents and Settings\Admin\Application
 Opens:
Data\Sun\Java\Deployment\security\java.policy
                          C:\Program Files\Java\jre7\lib\management
 Opens:
                         C:\WINDOWS\Fonts\coure.fon
 Opens:
                          C:\WINDOWS\Fonts\sserife.fon
 Opens:
                          C:\WINDOWS\Fonts\vgafix.fon
                          C:\Program Files\Java\jre7\lib\fonts
 Opens:
 Opens:
                          C:\Program Files\Java\jre7\bin\fontmanager.dll
 Opens:
                          C:\Program Files\Java\jre7\lib\fontconfig.bfc
 Opens:
                          C:\WINDOWS\Fonts
 Opens:
                          C:\Program Files\Java\jre7\lib\applet
 Opens:
                          C:\WINDOWS\Sun\Java\Deployment
 Opens:
                          C:\Program Files\Java\jre7\lib\currency.data
 Opens:
                          C:\WINDOWS\Temp\test12.jar.exe
 Opens:
                          C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\security
 Opens:
                          C:\Program Files\Java\jre7\lib\security\blacklist
 Opens:
                          C:\Program Files\Java\jre7\lib\security\trusted.libraries
                          C:\Program Files\Java\jre7\lib\jsse.jar
 Opens:
 Opens:
                          C:\WINDOWS\Fonts\arial.ttf
 Opens:
                          C:\Program Files\Java\jre7\bin\t2k.dll
                          C:\WINDOWS\Fonts\wingding.ttf
 Opens:
 Opens:
                          C:\WINDOWS\Fonts\symbol.ttf
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Active\RecoveryStore.{3AF75143-F55E-11E5-AE32-
08002719344D}.dat
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\~DF321B.tmp
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Microsoft\Internet Explorer\Recovery\Active\{3AF75145-F55E-11E5-AE32-08002719344D\}.dat
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\~DF35CE.tmp
                          C:\Documents and Settings\Admin\Local
 Writes to:
Settings\History\History.IE5\MSHist012016032920160330\index.dat
 Writes to:
                         C:\WINDOWS\system32\d3d9caps.tmp
 Reads from:
                          C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf
 Reads from:
                          C:\AUTOEXEC.BAT
 Reads from:
                          C:\WINDOWS\Registration\R00000000007.clb
 Reads from:
                          C:\WINDOWS\system32\url.dll
 Reads from:
                          C:\Documents and Settings\Admin\Favorites\Desktop.ini
 Reads from:
                          C:\WINDOWS\system32\oleacc.dll
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\$^DF321B.tmp}
 Reads from:
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Active\RecoveryStore.{3AF75143-F55E-11E5-AE32-
08002719344D}.dat
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\~DF35CE.tmp
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\Recovery\Active\{3AF75145-F55E-11E5-AE32-08002719344D}.dat
 Reads from:
                          C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
 Reads from:
                          C:\WINDOWS\Temp\test12.jar.html
 Reads from:
                          C:\WINDOWS\system32\ieframe.dll
                          C:\WINDOWS\system32\stdole2.tlb
 Reads from:
 Reads from:
                          C:\Program Files\Java\jre7\lib\meta-index
 Reads from:
                          C:\Program Files\Java\jre7\bin\client\classes.jsa
 Reads from:
                          C:\Program Files\Java\jre7\lib\rt.jar
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
 Reads from:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Microsoft\Internet Explorer\frameiconcache.dat
 Reads from:
                          C:\Program Files\Java\jre7\lib\deploy.jar
 Reads from:
                          C:\Program Files\Java\jre7\lib\javaws.jar
 Reads from:
                          C:\Program Files\Java\jre7\lib\plugin.jar
 Reads from:
                          C:\WINDOWS\system32\rsaenh.dll
                          {\tt C:\Program\ Files\Java\jre7\lib\ext\meta-index}
 Reads from:
 Reads from:
                          C:\Documents and Settings\Admin\Application
Data\Sun\Java\Deployment\deployment.properties
 Reads from:
                          C:\Program Files\Java\jre7\lib\security\java.security
 Reads from:
                          C:\WINDOWS\Prefetch\JAVA.EXE-1E21D4DA.pf
 Reads from:
                          C:\Program Files\Java\jre7\lib\i386\jvm.cfg
 Reads from:
                          C:\WINDOWS\system32\d3d9caps.dat
 Reads from:
                          C:\Program Files\Java\jre7\lib\net.properties
 Reads from:
                          C:\Program Files\Java\jre7\lib\security\java.policy
 Reads from:
                          C:\Program Files\Java\jre7\lib\fontconfig.bfc
 Reads from:
                          C:\Program Files\Java\jre7\lib\currency.data
 Reads from:
                          C:\WINDOWS\Temp\test12.jar.exe
 Reads from:
                          C:\Program Files\Java\jre7\lib\security\blacklist
 Reads from:
                          C:\Program Files\Java\jre7\lib\security\trusted.libraries
                          C:\Program Files\Java\jre7\lib\jsse.jar
 Reads from:
 Reads from:
                          C:\WINDOWS\Fonts\arial.ttf
```

Reads from: C:\WINDOWS\Fonts\wingding.ttf
Reads from: C:\WINDOWS\Fonts\symbol.ttf

Deletes: C:\Documents and Settings\Admin\Local Settings\History\History.IE5\MSHist012014033120140407\index.dat Deletes: C:\Documents and Settings\Admin\Local

Settings\History\History.IE5\MSHist012014033120140407
Deletes: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\MSHist012014041220140413\index.dat
Deletes: C:\Documents and Settings\Admin\Local

Settings\History\History.IE5\MSHist012014041220140413

Deletes: C:\WINDOWS\system32\d3d9caps.dat

Deletes: C:\WINDOWS\system32\d3d9caps.tmp

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

settings\connections

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

 ${\tt Creates \ key:} \qquad \qquad {\tt HKCU \setminus software \setminus microsoft \setminus windows \setminus current \ version \setminus internet \ settings \setminus zones}$

Creates key:

806d6172696f}\

Creates key: HKLM\software\microsoft\tracing

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

folders

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

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

Creates key: $\label{lem:hkculsoftware} \begin{tabular}{lll} HKCU\software\microsoft\trenet explorer\ecovery\active explorer\ecovery\trenet explorer\ecovery\active explorer\ecovery\trenet explorer\ecovery\active explorer\ecovery\ecover\ecovery\ecover\ecover\eco$

Creates key: HKCU\software

Creates key: HKCU\software\microsoft
Creates key: HKCU\software\microsoft\ctf
Creates key: HKCU\software\microsoft\ctf\tip

Creates key: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}

Creates key: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-

c9633f71be64}\languageprofile

Creates key: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-

 $c9633f71be64\\ \\ \\ language profile \\ \\ 0x00000000$

 $\label{lem:condition} \begin{tabular}{ll} Creates key: & HKCU \software \microsoft \internet explorer \min \windows search \end{tabular}$

Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{e2e2dd38-d088-

4134-82b7-f2ba38496583}\iexplore

Creates key: HKCU\software\microsoft\internet

explorer\lowregistry\extensions\cmdmapping

Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{fb5f1910-f110-

11d2-bb9e-00c04f795683}\iexplore

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

Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-

4283-a596-fa578c2ebdc3}\iexplore

Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-

435b-bc74-9c25c1c588a9}\iexplore

Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}

Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcba}\inprocserver32

Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}

Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcbb}\inprocserver32

Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}

Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcbc}\inprocserver32

Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-abcdeffedcba}

Creates key: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-

abcdeffedcba}\inprocserver32

Creates key: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}

Creates key: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-

00805f499d93}\inprocserver32

Creates key: HKCU\software\classes\javaplugin.1020
Creates key: HKCU\software\classes\javaplugin.1020\clsid

Creates key: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-

11cf-aaa5-00401c608501}\iexplore

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

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

settings\5.0\cache\extensible cache\mshist012016032920160330

Creates key: HKCU\software\microsoft\direct3d\mostrecentapplication 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\iexplore.exe Opens key: HKLM\system\currentcontrolset\control\terminal server HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\secur32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon Opens key: HKLM\ Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: 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\system\currentcontrolset\control\safeboot\option Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\kernel32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\shlwapi.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\iertutil.dll Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\oleaut32.dll Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.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: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ compatibility 32$ Opens kev: HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: HKLM\software\microsoft\windows nt\currentversion\windows Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance Opens key: HKLM\svstem\setup Opens key: HKCU\ Opens key: HKCU\software\policies\microsoft\control panel\desktop HKCU\control panel\desktop Opens kev: Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll Opens key: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ advanced$ Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack Opens key: HKLM\software\microsoft\ole Opens key: HKCR\interface Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046} Opens key: HKLM\software\microsoft\oleaut Opens key: HKLM\software\microsoft\oleaut\userera Opens key: HKCU\software\classes\ HKCU\software\classes\protocols\name-space handler\ Opens key: Opens key: HKCR\protocols\name-space handler HKCU\software\classes\protocols\name-space handler Opens kev: Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings Opens kev: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\

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

```
Opens key:
                         HKLM\software\microsoft\internet explorer\main\featurecontrol
 Opens key:
                         HKCU\software\microsoft\internet explorer\main\featurecontrol
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
 Opens kev:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\zonemap\domains\
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zonemap\ranges\
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
 Opens key:
                         HKLM\system\currentcontrolset\control\wmi\security
 Opens key:
                         HKLM\software\microsoft\internet explorer\main
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enablesafesearchpath_kb963027
 Opens kev:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enablesafesearchpath_kb963027
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ieframe.dll
 Opens key:
                         HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe
 Opens key:
                         HKLM\software\microsoft\internet explorer\setup
 Opens key:
                         HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-
0000c05bae0b}\typelib
 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
                         HKCR \land face \land \{79 eac9c4-baf9-11ce-8c82-00aa004ba90b\} \land proxystubclsid 32
 Opens key:
 Opens key:
                         HKCU\software\classes\interface\{000214e6-0000-0000-c000-
{\tt 000000000046} \verb|\proxystubclsid32| \\
                         Opens key:
                         HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-
 Opens kev:
00c04f79abd1}\proxystubclsid32
                         HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32
 Opens kev:
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer
 Opens key:
                         HKCU\software\microsoft\internet explorer
 Opens kev:
                         HKLM\software\microsoft\internet explorer
 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\wininet.dll
                         HKCU\software\microsoft\windows\currentversion\internet settings
 Opens key:
                         HKLM\software\policies
 Opens key:
                         HKCU\software\policies
 Opens key:
 Opens key:
                         HKCU\software
                         HKLM\software
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\main
 Opens key:
 Opens key:
                         HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\5.0\cache
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache\content
                         HKLM\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\content
 Opens key:
                         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 key:
settings\5.0\cache\history
```

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

 $\label{lem:hklm} \mbox{HKLM} \mbox{$\tt M$} \mbox{$\tt M$}$

options\iexplore.exe\rpcthreadpoolthrottle

HKLM\software\policies\microsoft\windows nt\rpc

Opens key:

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

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

```
settings\5.0\cache\extensible cache
                                    HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\domstore
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\feedplat
  Opens key:
                                    \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
settings\5.0\cache\extensible cache\iecompat
                                    \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Opens key:
settings\5.0\cache\extensible cache\ietld
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
                                    HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\privacie:
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature bufferbreaking 818408
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:
                                    HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                                     HKCU\software\microsoft\internet
  Opens key:
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
                                    HKCU\software\microsoft\internet
  Opens key:
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
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                                    HKLM\software\microsoft\internet
  Opens key:
\verb|explorer\main\featurecontrol\feature\_allow\_long\_international\_file names| \\
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                                    HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
                                    HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
                                     \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
  Opens key:
options\ws2help.dll
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options\ws2_32.dll
  Opens key:
                                     HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 0000000000001) \ (catalog\_entries \ (catalog \ (catalog\_entries \ (catalog \ (cata
  Opens key:
```

```
Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap col_catalog \\ \setminus catalog \\ \setminus
    Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
    Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
    Opens key:
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
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
    Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
                                                       \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\wpad}} \\
    Opens key:
                                                       HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                                                       HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                                                      HKU\
    Opens kev:
                                                       HKCU\software\microsoft\internet explorer\main
    Opens key:
    Opens key:
                                                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
    Opens key:
                                                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
   Opens kev:
                                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
```

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562

Opens key: HKLM\software\policies\microsoft\internet explorer\safety\privacie Opens key: HKCU\software\microsoft\internet explorer\safety\privacie

HKLM\software\microsoft\internet explorer\safety\privacie Opens kev: Opens key: HKCU\software\microsoft\internet explorer\new windows Opens key: HKLM\software\microsoft\internet explorer\new windows Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution options\comdlg32.dll

Opens key:

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

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

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

Opens key: HKLM\software\microsoft\ctf\

Opens key: HKLM\system\currentcontrolset\control\lsa Opens key: HKCU\software\microsoft\internet explorer\sqm Opens key: HKLM\software\microsoft\internet explorer\sqm Opens key: HKLM\software\microsoft\windows\currentversion

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

options\sqmapi.dll

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

options\xpsp2res.dll

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

HKCU\software\microsoft\internet Opens kev:

explorer\browseremulation\clearablelistdata

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

Opens key:

Opens key: HKCU\software\microsoft\internet explorer\toolbars\restrictions Opens key: HKLM\software\microsoft\internet explorer\toolbars\restrictions Opens kev: HKLM\software\microsoft\windows\currentversion\explorer\browser helper

objects

 $\label{lem:hklm} \verb+ Kklm \+ software + microsoft + internet explorer + extension$ Opens key:

compatibility\{18df081c-e8ad-4283-a596-fa578c2ebdc3}

HKCU\software\microsoft\windows\currentversion\ext\settings\{18df081c-Opens key:

e8ad-4283-a596-fa578c2ebdc3}

Opens key: $HKLM \ software \ microsoft \ windows \ current version \ ext \ settings \ \{18df081c-microsoft\} \ description \ ext \ description \ descript$

e8ad-4283-a596-fa578c2ebdc3}

HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3} Opens key: Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3} Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596fa578c2ebdc3}\treatas Opens kev: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\treatas Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596fa578c2ebdc3}\inprocserver32 HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserver32 Opens key: Opens key: HKLM\software\microsoft\internet explorer\extension compatibility\{dbc80044-a445-435b-bc74-9c25c1c588a9} $HKCU \ software \ microsoft \ windows \ current version \ ext \ settings \ \{dbc80044-dbc800404-dbc800404-dbc800404-dbc800404-dbc800404-dbc8004-dbc8004-dbc8004-dbc8004-dbc8004-dbc8004-dbc8004-dbc8004-dbc8004-d$ Opens key: a445-435b-bc74-9c25c1c588a9} Opens key: $HKLM \ software \ microsoft \ windows \ current version \ ext \ settings \ \ \{dbc 80044-dbc 80$ a445-435b-bc74-9c25c1c588a9} Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9} HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9} Opens key: Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\treatas Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\treatas Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserver32 Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserver32 Opens kev: HKLM\software\microsoft\internet explorer\toolbar Opens key: HKLM\software\policies\microsoft\internet explorer\security Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\ Opens key: $\label{lem:hkcu} \mbox{\current} windows \mbox{\current} internet settings \mbox{\current} settings \mbox{\current} and \mbo$ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2 HKCU\software\microsoft\windows\currentversion\internet settings\zones\3 Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\ Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zones\0 HKCU\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zones\0 HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\1 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zones\1 Opens kev: HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\ HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zones\2 Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}$ 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 $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} explicitly independent of the local property of the local propert$ Opens key: settings\lockdown_zones\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\lockdown_zones\ HKCU\software\microsoft\windows\currentversion\internet 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\0 HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\0 Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\lockdown_zones\0 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\1 HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\lockdown_zones\1 Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}$ settings\lockdown_zones\1 Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}$ settings\lockdown_zones\2 HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\lockdown_zones\2

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

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

Opens key:

Opens key:

settings\lockdown_zones\2

settings\lockdown_zones\3 HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\lockdown_zones\3 $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\lockdown_zones\3 Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4 HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\4 HKCU\software\policies\microsoft\windows\currentversion\internet Opens key: settings\lockdown_zones\4 Opens key: HKCU\software\microsoft\internet explorer\security Opens key: HKLM\software\microsoft\internet explorer\security Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069a2d8-08002b30309d} Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32 Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32 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 HKLM\software\microsoft\windows\currentversion\setup Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: HKLM\software\policies\microsoft\system\dnsclient Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume Opens key: 11e3-9fc7-806d6172696f}\ HKCU\software\classes\drive\shellex\folderextensions Opens key: Opens key: HKCR\drive\shellex\folderextensions Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9} Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9} HKCU\software\classes\directory Opens key: Opens key: HKCR\directory Opens key: HKCU\software\classes\directory\curver Opens key: HKCR\directory\curver Opens key: HKCR\directorv\ Opens key: HKCU\software\microsoft\windows\currentversion\explorer Opens key: HKCU\software\microsoft\windows\currentversion\explorer\ Opens key: HKCU\software\microsoft\windows\currentversion\policies\system HKCU\software\classes\directory\shellex\iconhandler Opens kev: HKCR\directory\shellex\iconhandler Opens key: Opens key: HKCU\software\classes\directory\clsid Opens key: HKCR\directory\clsid HKCU\software\classes\folder Opens key: Opens key: HKCR\folder Opens kev: 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\.html HKCU\software\classes\.html Opens key: Opens key: HKCR\.html Opens key: HKCU\software\classes\htmlfile Opens key: HKCR\htmlfile Opens key: HKCU\software\classes\htmlfile\curver Opens key: HKCR\htmlfile\curver HKCR\htmlfile\ Opens key: Opens key: HKCU\software\classes\htmlfile\shellex\iconhandler Opens key: HKCR\htmlfile\shellex\iconhandler HKCU\software\classes\systemfileassociations\.html Opens key: Opens key: HKCR\systemfileassociations\.html Opens key: HKCU\software\classes\systemfileassociations\text HKCR\systemfileassociations\text Opens key: Opens key: HKCU\software\classes\htmlfile\clsid Opens key: HKCR\htmlfile\clsid $HKCU \setminus software \setminus classes \setminus clsid \setminus \{25336920-03f9-11cf-8fd0-11c$ Opens key: 00aa00686f13}\implemented categories\{00021490-0000-0000-c000-000000000046} Opens kev:

categories\{00021490-0000-0000-0000-000000000046}

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

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

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

Opens key: HKLM\software\policies\microsoft\vindows\safer\levelobjects

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\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\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
    Opens key:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe
b91490411bfc}
    Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
    Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
    Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
    Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
    Opens kev:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus urlzones
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
    Opens kev:
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
    Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                                                                   HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
    Opens kev:
                                                                   \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \node \node
    Opens key:
    Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \normalfooth \code identifiers \normalfooth \code identifiers \normalfooth \code identifiers \normalfooth \code \
    Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
    Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
    Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus urlzones
   Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
    Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus paths
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
    Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus paths
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                                                                   HKCU\software\microsoft\windows\currentversion\explorer\shell folders
    Opens kev:
    Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options\rasman.dll
    Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rtutils.dll
```

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

HKLM\software\microsoft\windows nt\currentversion\drivers32

Opens key:

Opens key:

options\winmm.dll
 Opens key:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm

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

options\tapi32.dll

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

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

options\rasapi32.dll

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

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

options\userenv.dll

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

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

folders

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\system\currentcontrolset\control\session manager\environment
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-211757981266-507921405-1957994488-1003

Opens key: HKCU\environment

Opens key: HKCU\volatile environment

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

options\sensapi.dll

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

options\msimg32.dll

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

options\ieui.dll

Opens key: HKLM\software\microsoft\directui

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

Opens key: HKCU\software\microsoft\internet explorer\recovery
Opens key: HKLM\software\microsoft\internet explorer\recovery

Opens key: HKLM\software\microsoft\com3

Opens key: HKCU\software\classes\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}

Opens key: HKCR\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}
Opens key: HKCU\software\classes\interface\{1ac7516e-e6bb-4a69-b63f-

e841904dc5a6}\proxystubclsid32

Opens key: HKCR\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}\proxystubclsid32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\comres.dll

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

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\{a4a1a128-768f-41e0-bf75-

e4fddd701cba}\treatas
Opens kev:

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

 Opens key:
 HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75

e4fddd701cba}\inprocserver32

Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32

Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-

e4fddd701cba}\inprocserverx86

 $Opens~key: \\ HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\\\ \ inprocserverx86$

Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-

e4fddd701cba}\localserver32

Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\localserver32

Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-

e4fddd701cba}\inprochandler32

 $Opens~key: \\ HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\\\ \ inprochandler 32$

Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-

e4fddd701cba}\inprochandlerx86

Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-

e4fddd701cba}\localserver

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

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

options\ieproxy.dll

Opens key: HKCU\software\classes\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}

Opens key: $\label{lem:hkcn} \begin{tabular}{ll} HKCR \end{tabular} HKCU \end{tabular} HKCU \end{tabular} HKCU \end{tabular} HKCU \end{tabular} HKCU \end{tabular} HKCU \end{tabular} HCU \end{$

Opens key: HKCR\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}\proxystubclsid32
Opens key: HKLM\software\policies\microsoft\internet explorer\tabbedbrowsing
Opens key: HKCU\software\microsoft\internet explorer\tabbedbrowsing

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

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

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

f4ceaaf59cfc}\treatas Opens key:

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

f4ceaaf59cfc}\inprocserver32

Opens kev: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32

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

f4ceaaf59cfc}\inprocserverx86

HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserverx86 Opens key:

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

f4ceaaf59cfc}\localserver32

Opens key: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver32

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

f4ceaaf59cfc}\inprochandler32

HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandler32 Opens key:

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

f4ceaaf59cfc}\inprochandlerx86

HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprochandlerx86 Opens kev:

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

f4ceaaf59cfc}\localserver

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

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

options\msimtf.dll

Opens kev: HKLM\software\microsoft\ctf\tip

Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-

c9633f71be64}\languageprofile

 $HKCU \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 80$ Opens key:

c9633f71be64}\languageprofile

HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-Opens key:

c9633f71be64}\languageprofile\0x00000000

Opens key: $HKCU \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8$ c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}

HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53} Opens key:

Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53} Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-

431b3828ba53}\treatas

Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-Opens kev:

431b3828ba53}\inprocserver32

HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32 Opens key:

HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-Opens key:

431b3828ba53}\inprocserverx86

HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86 Opens key:

HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-Opens kev:

431b3828ba53}\localserver32

HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32 Opens kev: Opens key: HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-

431b3828ba53}\inprochandler32

Opens key: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandler32

HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-Opens kev:

431b3828ba53}\inprochandlerx86

HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86 Opens key:

HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-Opens key:

431b3828ba53}\localserver

HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7} Opens key:

HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7} Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-Opens key:

869523e2d6c7}\treatas

HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\inprocserver32

Opens key: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32

Opens key:

869523e2d6c7}\inprocserverx86

HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserverx86 Opens key:

HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-Opens kev:

869523e2d6c7}\localserver32

HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver32 Opens key:

Opens key:

869523e2d6c7}\inprochandler32

 $HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\ \ \ in prochandler 32$ Opens key:

HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-Opens kev:

869523e2d6c7}\inprochandlerx86

HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86 Opens key:

Opens key: HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\localserver

Opens key: $\label{localserver} $HKCR \cdot a_4b_544a_1-438d-4b_41-9325-869523e_2d_6c_7 \cdot localserver $$ f(a_4b_544a_1-438d-4b_41-9325-869523e_2d_6c_7) $$ f(a_4b_544a_1-438d-4b_41-4b$ Opens key: HKCU\software\policies\microsoft\internet explorer\main

HKLM\software\microsoft\ctf\tip\ Opens kev:

Opens key:

c9633f71be64}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}

HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-Opens kev:

```
HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
      Opens key:
e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                              HKLM \setminus software \setminus irrosoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-
      Opens key:
00c04fc324a1}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
      Opens kev:
                                                                                             HKLM \setminus software \setminus microsoft \setminus tip \setminus \{f89e9e58-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2
0 f816 c09 f4 ee \} \\ category \\ \{b95 f181 b-ea4 c-4 af1-8056-7 c321 abbb091\}
      Opens key:
                                                                                              HKCU\software\microsoft\ctf\langbaraddin\
                                                                                              HKLM\software\microsoft\ctf\langbaraddin\
      Opens key:
      Opens key:
                                                                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpshims.dll
      Opens key:
                                                                                              HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
      Opens key:
                                                                                              HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
      Opens key:
                                                                                              HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                              HKLM \setminus software \setminus microsoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143-b5b1-143
      Opens key:
00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
     Opens key:
                                                                                              HKLM \setminus software \setminus microsoft \setminus tip \setminus \{f89e9e58-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2f-4008-9ac2-bd2
Of816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
      Opens key:
                                                                                              c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                                             HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
      Opens kev:
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
     Opens key:
                                                                                              HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
      Opens key:
                                                                                              HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                                             HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 80
      Opens key:
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
     Opens key:
                                                                                             HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
      Opens key:
                                                                                              HKCU \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - c9633f71be64\}
      Opens key:
                                                                                              HKCU\software\microsoft\internet explorer\main\windowssearch
      Opens key:
                                                                                              HKLM\software\policies\microsoft\internet explorer\feeds
      Opens key:
                                                                                              HKCU\software\microsoft\internet explorer\feeds
      Opens key:
                                                                                              HKLM\software\microsoft\internet explorer\feeds
      Opens key:
                                                                                              HKCU\software\classes\.url\persistenthandler
      Opens key:
                                                                                              HKCR\.url\persistenthandler
      Opens key:
                                                                                              HKLM\software\policies\microsoft\internet explorer\main\windowssearch
                                                                                              HKLM\software\microsoft\windows search
      Opens key:
      Opens key:
                                                                                              HKLM\software\policies\microsoft\internet explorer\toolbar\webbrowser
      Opens key:
                                                                                              HKCU\software\microsoft\internet explorer\toolbar\webbrowser
                                                                                              \label{lem:hklm} \verb+Kklm \+ software + microsoft + internet explorer + toolbar + webbrowser
      Opens key:
      Opens key:
                                                                                              HKCU\software\microsoft\windows\currentversion\policies\ieak
      Opens key:
                                                                                              HKLM\software\microsoft\windows\currentversion\policies\ieak
                                                                                              \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
      Opens key:
options\uxtheme.dll
                                                                                              HKCU\software\microsoft\windows\currentversion\thememanager
      Opens kev:
      Opens key:
                                                                                              HKLM\software\policies\microsoft\internet explorer\commandbar
      Opens key:
                                                                                              HKCU\software\microsoft\internet explorer\commandbar
      Opens key:
                                                                                              HKLM\software\microsoft\internet explorer\commandbar
      Opens key:
                                                                                              HKLM\software\microsoft\windows\currentversion\explorer
      Opens key:
                                                                                              HKLM\software\microsoft\windows\currentversion\explorer\
      Opens kev:
                                                                                              HKCU\control panel\desktop\windowmetrics
      Opens key:
                                                                                              HKLM\software\microsoft\windows\currentversion\explorer\shell icons
      Opens kev:
Opens key:
HKLM \label{liconoverlay} HKLM \label{liconoverlay} Which is a substitution of the s
     Opens key:
                                                                                             HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprocserver32
      Opens key:
                                                                                              HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserver32
      Opens key:
                                                                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
      Opens key:
                                                                                              HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}
      Opens key:
                                                                                              HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}
                                                                                              HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
      Opens key:
080036587f03}\treatas
      Opens key:
                                                                                              HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\treatas
                                                                                              HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
      Opens key:
080036587f03}\inprocserverx86
      Opens key:
                                                                                              HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserverx86
                                                                                              HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
      Opens key:
080036587f03}\localserver32
                                                                                              HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\localserver32
      Opens kev:
      Opens key:
                                                                                              HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprochandler32
      Opens key:
                                                                                              HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprochandler32
      Opens key:
                                                                                              HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprochandlerx86
                                                                                             HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprochandlerx86
      Opens kev:
      Opens key:
                                                                                              HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
```

```
080036587f03}\localserver
                                                                     HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\localserver
    Opens kev:
    Opens key:
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cscdll.dll
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens kev:
options\cscui.dll
                                                                      HKCU \setminus software \setminus classes \setminus clsid \setminus \{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7\}
    Opens key:
                                                                      HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}
    Opens key:
    Opens key:
                                                                      HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\treatas
                                                                      HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\treatas
    Opens key:
    Opens key:
                                                                      HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\inprocserver32
                                                                     HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32
    Opens key:
    Opens key:
                                                                      HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\inprocserverx86
                                                                     HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserverx86
    Opens kev:
    Opens key:
                                                                      HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\localserver32
                                                                     HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\localserver32
    Opens key:
    Opens key:
                                                                      HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\inprochandler32
                                                                      HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandler32
    Opens kev:
    Opens key:
                                                                      HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\inprochandlerx86
                                                                     HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprochandlerx86
    Opens key:
    Opens key:
                                                                     HKCU\software\classes\clsid\{b5f8350b-0548-48b1-a6ee-
88bd00b4a5e7}\localserver
    Opens key:
                                                                     HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\localserver
    Opens key:
                                                                      HKCU\software\classes\appid\{667524be-9ec0-4196-91c9-c6ed1f7a899d}
    Opens key:
                                                                      HKCR\appid\{667524be-9ec0-4196-91c9-c6ed1f7a899d}
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options\msvcp60.dll
    Opens key:
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleacc.dll
    Opens key:
                                                                      HKLM\software\microsoft\active accessibility\handlers
    Opens key:
                                                                      HKCU\software\classes\typelib
                                                                      HKCR\typelib
    Opens key:
    Opens key:
                                                                      HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}
    Opens key:
                                                                      HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}
                                                                      HKCU \setminus software \\ classes \setminus typelib \setminus \{1ea4dbf0-3c3b-11cf-810c-00aa00389b71\} \\ \setminus 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1.1 + 1
    Opens key:
    Opens key:
                                                                      HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71\}\1.1
                                                                      HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
    Opens kev:
00aa00389b71}\1.1\flags
                                                                      HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\flags
    Opens kev:
    Opens key:
                                                                      HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
00aa00389b71}\1.1\0
    Opens key:
                                                                      HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0
                                                                      HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
    Opens kev:
00aa00389b71}\1.1\0\win32
                                                                      HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0\win32
    Opens key:
                                                                     HKCU\software\classes\typelib\{1ea4dbf0-3c3b-11cf-810c-
    Opens key:
00aa00389b71}\1.1\helpdir
                                                                      \label{lem:hkcr} $$HKCR\times typelib = 4dbf0-3c3b-11cf-810c-00aa00389b71 - 1.1 + elpdir = 1.0 + el
    Opens key:
    Opens kev:
                                                                      HKCU\software\classes\interface
    Opens key:
                                                                      HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}
                                                                      HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}
    Opens key:
    Opens key:
                                                                      HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid
    Opens key:
                                                                      HKCR\ \ terface \ \ \{618736e0-3c3d-11cf-810c-00aa00389b71\} \ \ \ \ \ tubclsid
    Opens key:
                                                                      HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
                                                                      HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid32
    Opens key:
    Opens key:
                                                                      HKCU\software\classes\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\typelib
    Opens key:
                                                                      HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\typelib
    Opens key:
                                                                      HKCU\software\classes\interface\{03022430-abc4-11d0-bde2-00aa001a1953}
                                                                      HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}
    Opens key:
    Opens key:
                                                                      HKCU \setminus software \setminus classes \setminus interface \setminus \{03022430 - abc4 - 11d0 - bde2 - abc4 - abc4
00aa001a1953}\proxystubclsid
                                                                      HKCR \verb|\| interface \verb|\| \{03022430-abc4-11d0-bde2-00aa001a1953\} \verb|\| proxystubclsid| | the content of the con
    Opens key:
    Opens key:
                                                                      HKCU\software\classes\interface\{03022430-abc4-11d0-bde2-
00aa001a1953}\proxystubclsid32
                                                                     HKCR \verb|\| interface \verb|\| \{03022430-abc4-11d0-bde2-00aa001a1953\} \verb|\| proxystubclsid32| 
    Opens key:
    Opens key:
                                                                      HKCU\software\classes\interface\{03022430-abc4-11d0-bde2-
00aa001a1953}\typelib
    Opens key:
                                                                      HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\typelib
    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
```

HKCU\software\microsoft\windows\currentversion\internet

Opens key:

settings\zonemap\ranges\

```
Opens key:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
   Opens key:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                                                        HKLM\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\domains\
   Opens key:
                                                         HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com
   Opens key:
                                                         HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com\related
                                                        HKCU\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
   Opens key:
                                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\ietld
   Opens key:
                                                         HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
   Opens key:
                                                        HKLM\software\policies\microsoft\internet
explorer\infodelivery\restrictions
   Opens key:
                                                        HKCU\software\policies\microsoft\internet
explorer\infodelivery\restrictions
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\searchurl
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\searchscopes
                                                         HKLM\software\microsoft\internet explorer\searchscopes
   Opens kev:
   Opens key:
                                                         HKLM\software\policies\microsoft\internet
explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}
                                                        HKCU\software\policies\microsoft\internet
   Opens key:
explorer\searchscopes\{0633ee93-d776-472f-a0ff-e1416b8b2e3a}
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}
   Opens key:
                                                         HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}
                                                         HKLM\software\policies\microsoft\internet explorer\searchscopes
   Opens key:
   Opens key:
                                                         HKLM\software\policies\microsoft\internet explorer\toolbar
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\toolbar
                                                         \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\internet explorer\toolbars\restrictions}}
   Opens key:
   Opens key:
                                                         HKLM\software\policies\microsoft\internet explorer\linksbar
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\linksbar
                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\xmllite.dll
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\extensions
                                                         HKLM\software\microsoft\internet explorer\extensions
   Opens key:
   Opens key:
                                                         HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-
4134-82b7-f2ba38496583}
                                                        HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_addon_management
                                                        HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_addon_management
   Opens key:
                                                         \label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \slightly policies \ext \clsid
                                                         HKCU\software\microsoft\windows\currentversion\policies\ext\clsid
   Opens kev:
   Opens key:
                                                         HKLM\software\microsoft\windows\currentversion\policies\ext
   Opens key:
                                                         HKCU\software\microsoft\windows\currentversion\policies\ext
                                                         \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc}(e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38
   Opens key:
d088-4134-82b7-f2ba38496583}
                                                         HKLM \ software \ microsoft \ windows \ current version \ ext \ settings \ \{e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd38-e2e2dd
   Opens key:
d088-4134-82b7-f2ba38496583}
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-
4134-82b7-f2ba38496583}
   Opens key:
                                                         HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-
4134-82b7-f2ba38496583}\lang0409
                                                         Opens key:
11d2-bb9e-00c04f795683}
                                                         HKCU \ software \ microsoft \ windows \ current version \ ext \ settings \ \{fb5f1910-microsoft\} \ description \ ext \ description \ descript
   Opens key:
f110-11d2-bb9e-00c04f795683}
                                                         HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{fb5f1910-the articles \} 
   Opens kev:
f110-11d2-bb9e-00c04f795683}
                                                         HKCU\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
   Opens key:
11d2-bb9e-00c04f795683}
                                                         Opens key:
11d2-bb9e-00c04f795683}\lang0409
   Opens key:
                                                         HKLM\software\policies\microsoft\internet explorer\restrictions
   Opens key:
                                                         HKCU\software\policies\microsoft\internet explorer\restrictions
   Opens key:
                                                         HKLM\software\policies\microsoft\internet explorer\iedevtools
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\iedevtools
   Opens key:
                                                         HKLM\software\microsoft\internet explorer\iedevtools
   Opens key:
                                                         HKCU\software\microsoft\internet explorer\lowregistry\commandbar
                                                         HKCU\software\microsoft\internet explorer\linksexplorer
   Opens kev:
                                                         HKLM\software\microsoft\internet explorer\linksexplorer
   Opens key:
   Opens key:
                                                         HKCU\software\classes\clsid\{0002df01-0000-0000-c000-00000000046}
   Opens key:
                                                         HKCR\clsid\{0002df01-0000-0000-c000-00000000046}
                                                         Opens key:
000000000046}\treatas
                                                         HKCR\clsid\{0002df01-0000-0000-c000-00000000046}\treatas
   Opens key:
```

HKCU\software\classes\clsid\{0002df01-0000-0000-c000-

Opens key:

```
00000000046}\inprocserver32
                         HKCR\clsid\{0002df01-0000-0000-c000-00000000046}\inprocserver32
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{0002df01-0000-0000-c000-
00000000046}\inprocserverx86
 Opens key:
                         HKCR\clsid\{0002df01-0000-0000-c000-00000000046}\inprocserverx86
```

Opens key: HKCU\software\classes\clsid\{0002df01-0000-0000-c000-

000000000046}\localserver32

HKCR\clsid\{0002df01-0000-0000-c000-00000000046}\localserver32 Opens key:

HKCU\software\classes\clsid\{0002df01-0000-0000-c000-Opens key:

00000000046}\inprochandler32

Opens kev: HKCR\clsid\{0002df01-0000-0000-c000-0000000046}\inprochandler32

HKCU\software\classes\clsid\{0002df01-0000-0000-c000-Opens key:

000000000046}\inprochandlerx86

HKCR\clsid\{0002df01-0000-0000-c000-0000000046}\inprochandlerx86 Opens key: Opens key: HKCU\software\classes\clsid\{3af75140-f55e-11e5-ae32-08002719344d} HKCR\clsid\{3af75140-f55e-11e5-ae32-08002719344d} Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e} Opens kev: Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}

Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-

b1deb82c6e5e}\treatas

Opens key: $HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\ \ treat as$ Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-

b1deb82c6e5e}\inprocserver32

Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\inprocserver32

Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-

b1deb82c6e5e}\inprocserverx86

Opens key:

HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-Opens key:

b1deb82c6e5e}\localserver32

Opens key: HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\localserver32

Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-

b1deb82c6e5e}\inprochandler32

Opens key:

Opens key: HKCU\software\classes\clsid\{d5e8041d-920f-45e9-b8fb-

b1deb82c6e5e}\inprochandlerx86

Opens key:

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

HKLM\system\currentcontrolset\control\securityproviders Opens key: Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll

HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll Opens key: Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key:

options\iphlpapi.dll

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

Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces

Opens kev: HKLM\svstem\currentcontrolset\services\netbt\parameters

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

options\msv1_0.dll

HKCU\software\classes\htmlfile\shellex\{000214f9-0000-0000-c000-Opens key:

00000000046}

Opens key: HKCR\htmlfile\shellex\{000214f9-0000-0000-c000-00000000046} Opens kev: HKCU\software\classes\.html\shellex\{000214f9-0000-0000-c000-

00000000046}

HKCR\.html\shellex\{000214f9-0000-0000-c000-00000000046} Opens key:

Opens key: HKCU\software\classes\systemfileassociations\text\shellex\{000214f9-

0000-0000-c000-000000000046}

Opens key:

000000000046}

HKCU\software\classes* Opens key:

Opens key: HKCR*

Opens key: HKCU\software\classes*\shellex\{000214f9-0000-0000-c000-000000000046}

HKCR*\shellex\{000214f9-0000-0000-c000-00000000046} Opens key:

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

history

 $\label{local-eq:hkcu} \begin{tabular}{ll} HKCU \software \classes \interface \ \{8a7476f4-d264-4e13-ae72-20cd9831d98c\} \end{tabular}$ Opens key:

Opens key: HKCR\interface\{8a7476f4-d264-4e13-ae72-20cd9831d98c} Opens key: HKCU\software\classes\interface\{8a7476f4-d264-4e13-ae72-

20cd9831d98c}\proxystubclsid32

Opens key: $HKCR \land (8a7476f4-d264-4e13-ae72-20cd9831d98c) \land (proxystubclsid32) \land ($ Opens key: HKCU\software\classes\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d}

HKCR\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d} Opens key: Opens key: HKCU\software\classes\interface\{b40c43f1-f039-44d2-aeb7-87f5af8abc3d}\proxystubclsid32

 $HKCR \ interface \ \{b40c43f1-f039-44d2-aeb7-87f5af8abc3d\} \ proxystubclsid32$ Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus interface \setminus \{d358f4e1-0465-4965-9dd5-cae303d2c345\}$ Opens key: HKCR\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}

Opens key: HKCU\software\classes\interface\{d358f4e1-0465-4965-9dd5-

cae303d2c345}\proxystubclsid32

HKCR\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}\proxystubclsid32 Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus interface \setminus \{ff18630e-5b18-4a07-8a75-9fd3ce5a2d14\}$ Opens key: HKCR\interface\{ff18630e-5b18-4a07-8a75-9fd3ce5a2d14\}
Opens key: HKCU\software\classes\interface\{ff18630e-5b18-4a07-8a75-

9fd3ce5a2d14}\proxystubclsid32

Opens key: HKCR\interface\{ff18630e-5b18-4a07-8a75-9fd3ce5a2d14}\proxystubclsid32 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\mlang.dll

Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-

fa578c2ebdc3}\inprocserverx86

Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-

fa578c2ebdc3}\localserver32

Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\localserver32

Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-

fa578c2ebdc3}\inprochandler32

Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprochandler32

Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-

fa578c2ebdc3}\inprochandlerx86

Opens key: HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{18df081c-e8ad-4283-a596-

fa578c2ebdc3}\localserver

Opens key: $\label{eq:hkclsid} $$ HKCR\clsid_{18df081c-e8ad-4283-a596-fa578c2ebdc3} \log e $$ Opens key: $$ HKCU\software\classes\appid_{77ab4812-5411-4ea9-8437-77ad0f230302} $$$

Opens key: HKCR\appid\{77ab4812-5411-4ea9-8437-77ad0f230302}

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

options\msvcr80.dll

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

options\msvcp80.dll

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

options\acroiehelpershim.dll

Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-

784b7d6be0b3}\inprocserver32

Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprocserver32
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\acroiehelper.dll

Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}

Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3\}
Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-

784b7d6be0b3}\treatas

Opens key: $\label{eq:hcclsid} \begin{tabular}{ll} HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\treat as \\ Opens key: \\ HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-784b7d5p-b87d-784b7d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b7d5p-b87d-784b$

784b7d6be0b3}\inprocserverx86

Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-

784b7d6be0b3}\localserver32

 $Opens~key: \\ HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\localserver 32$

Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-

 $784b7d6be0b3\\ \verb|\inprochandler32|$

Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprochandler32

Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-

784b7d6be0b3}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{06849e9f-c8d7-4d59-b87d-

784b7d6be0b3}\localserver

Opens key: HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\localserver

Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-

4283-a596-fa578c2ebdc3}\iexplore

Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-

9c25c1c588a9}\inprocserverx86

Opens key: $\label{eq:hkcr} \mbox{HKCR\clsid\dbc80044-a445-435b-bc74-9c25c1c588a9} \mbox{\label{eq:hkcr} inprocserverx86}$

Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-

9c25c1c588a9}\localserver32

Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\localserver32

Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-

 $9c25c1c588a9 \} \verb|\inprochandler32|$

 $Opens~key: \\ HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\\\ \ inprochandler 32$

Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-

9c25c1c588a9}\inprochandlerx86

Opens key: $\label{eq:hkcr_lsid} \begin{tabular}{ll} HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprochandlerx86. \end{tabular}$

Opens key: HKCU\software\classes\clsid\{dbc80044-a445-435b-bc74-

9c25c1c588a9}\localserver

Opens key: HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\localserver

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

options\msvcr100.dll

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

options\jp2ssv.dll

Opens key: HKLM\software\javasoft

Opens key: HKLM\software\javasoft\java plug-in
Opens key: HKLM\software\javasoft\java plug-in\10.2.0
Opens key: HKLM\software\javasoft\java plug-in\1.7.0_02
Opens key: HKLM\software\javasoft\java runtime environment

Opens key: HKLM\software\javasoft\java runtime environment\1.7.0_02

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

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcba}

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcba}\inprocserver32

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcbb}\inprocserver32

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcbc}\inprocserver32

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-abcdeffedcba}

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-

abcdeffedcba}\inprocserver32

Opens key: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}

Opens key: HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-

00805f499d93}\inprocserver32

Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}

Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}
Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-

00401c608501}\treatas

Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\treatas

Opens key: HKCU\software\classes\javaplugin.1020
Opens key: HKCU\software\classes\javaplugin.1020\clsid

Opens key: HKLM\software\mozilla

Opens key: HKLM\software\mozilla\mozilla firefox

Opens key: HKLM\software\mozilla.org

Opens key: HKCU\software\classes\htmlfile\shellex\{a39ee748-6a27-4817-a6f2-

13914bef5890}

Opens key: HKCR\htmlfile\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}
Opens key: HKCU\software\classes\.html\shellex\{a39ee748-6a27-4817-a6f2-

13914bef5890}

Opens key: HKCR\.html\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}

Opens key: HKCU\software\classes\systemfileassociations\text\shellex\{a39ee748-

6a27-4817-a6f2-13914bef5890}

Opens key: HKCR\systemfileassociations\text\shellex\{a39ee748-6a27-4817-a6f2-

13914bef5890}

Opens key: HKCU\software\classes*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}

Opens key: HKCR*\shellex\{a39ee748-6a27-4817-a6f2-13914bef5890}

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

Opens key: $\mbox{HKCU\software\mbox{\sm}icrosoft\internet\ explorer\suggested\ sites}$

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

options\sxs.dll

Opens key: HKCU\software\classes\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}

Opens key: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}

Opens key: HKCU\software\classes\typelib\{5f226421-415d-408d-9a09-

0dcd94e25b48}\1.0\0

0dcd94e25b48\1.0\0\win32

Opens key: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0\win32 Opens key: HKCU\software\microsoft\internet

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

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

000000000046}

Opens key: HKCR\htmlfile\shellex\{000214e6-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\.html\shellex\{000214e6-0000-0000-c000-

00000000046}

Opens key: HKCR\.html\shellex\{000214e6-0000-0000-c000-00000000046}

Opens key: HKCU\software\classes\systemfileassociations\text\shellex\{000214e6-

0000-0000-c000-000000000046}

Opens key: HKCR\systemfileassociations\text\shellex\{000214e6-0000-0000-c000-

000000000046}

Opens key: HKCU\software\classes*\shellex\{000214e6-0000-0000-c000-00000000046}

Opens key: HKCR*\shellex\{000214e6-0000-0000-c000-00000000046}

Opens key: HKLM\software\policies\microsoft\internet explorer\browseremulation
Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}

Opens key: $\label{eq:hkkcn} \begin{tabular}{ll} HKCR\clsid\footnote{\clsid} -0ac9-11d1-896c-00c04fb6bfc4} \\ Opens key: \\ HKCU\software\classes\clsid\footnote{\clsid} -7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4} \\ \end{tabular}$

00c04fb6bfc4}\treatas

00c04fb6bfc4}\inprocserver32

Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-

00c04fb6bfc4}\inprocserverx86

Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-

00c04fb6bfc4}\localserver32

Opens key: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\localserver32

Opens key: HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-

```
00c04fb6bfc4}\inprochandler32
                                    HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
  Opens key:
                                    HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-
  Opens kev:
00c04fb6bfc4}\inprochandlerx86
  Opens key:
                                    HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86
  Opens key:
                                    HKCU\software\classes\clsid\{7b8a2d95-0ac9-11d1-896c-
00c04fb6bfc4}\localserver
  Opens key:
                                    HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\localserver
  Opens kev:
                                    HKLM\software\microsoft\windows\currentversion\internet settings\zones\0
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_read_zone_strings_from_registry
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_read_zone_strings_from_registry
                                    HKLM\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
                                    HKLM\software\microsoft\internet explorer\mediatypeclass
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings\accepted documents
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\policies\ratings
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:
                                    HKCU\software\classes\protocols\name-space handler\about\
  Opens key:
                                    HKCR\protocols\name-space handler\about
  Opens key:
                                    HKCU\software\classes\protocols\name-space handler\*\
  Opens key:
                                    HKCR\protocols\name-space handler\*
  Opens key:
                                    HKCU\software\classes\protocols\handler\about
  Opens key:
                                    HKCR\protocols\handler\about
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\treatas
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\tinprocserver32
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
                                    HKCR \c1sid \c1os 6.05 - 11cf-bb82-00aa00bdce0b\c1os 6.05 - 11cf-bb82-00aa00bdce0b\c
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
                                    HKCR \verb|\clsid|{3050f406-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprochandler32| \\
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandlerx86
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\localserver
                                    HKCR \clsid \ \{3050f406-98b5-11cf-bb82-00aa00bdce0b\} \localserver
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msls31.dll
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\mshtml.dll
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
  Opens key:
                                    HKLM\software\microsoft\internet
```

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

```
explorer\main\featurecontrol\feature_private_font_setting
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_private_font_setting
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature css show hide events
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_display_node_advise_kb833311
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature body size in editable iframe kb943245
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_object_caching
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
                                    HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_cleanup_at_fls
                                    HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
  Opens kev:
                                    HKLM\software\microsoft\internet explorer\application compatibility
  Opens key:
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\domstorage
  Opens key:
                                    HKCU\software\microsoft\internet explorer\domstorage
                                    HKLM\software\microsoft\internet explorer\domstorage
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_mime_handling
  Opens key:
                                    HKCU\software\classes\protocols\name-space handler\file\
                                    HKCR\protocols\name-space handler\file
  Opens key:
  Opens key:
                                    HKCU\software\classes\protocols\filter\text/html
  Opens key:
                                    HKCR\protocols\filter\text/html
  Opens kev:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_safe_bindtoobject
  Opens key:
                                    HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
  Opens key:
                                    HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
  Opens key:
                                    HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\treatas
                                    HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
  Opens key:
  Opens key:
                                    HKCU \setminus software \setminus classes \setminus clsid \setminus \{25336920 - 03f9 - 11cf - 8fd0 - 11cf - 1
00aa00686f13}\inprocserver32
                                    HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
  Opens key:
                                    HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
  Opens key:
00aa00686f13}\inprocserverx86
                                    HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserverx86
  Opens kev:
  Opens key:
                                    HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver32
  Opens key:
                                    HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver32
```

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

00aa00686f13}\inprochandler32

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32

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

00aa00686f13}\inprochandlerx86

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandlerx86

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

00aa00686f13}\localserver

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver

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

options\psapi.dll

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

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

Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}

Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d\}
Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-

084657eddc7d}\treatas

Opens key: $\label{eq:hccl} \begin{tabular}{ll} HKCR\clsid\a6b222ab-a5ea-4899-b230-084657eddc7d\treatas \\ Opens key: \\ HKCU\software\classes\clsid\a6b222ab-a5ea-4899-b230-\\ \end{tabular}$

084657eddc7d}\inprocserver32

 $Opens~key: \\ HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\ \ \ inprocserver32$

Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-

084657eddc7d}\inprocserverx86

Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-

084657eddc7d}\localserver32

Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\localserver32

Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-

084657eddc7d}\inprochandler32

Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprochandler32

Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-

084657eddc7d}\inprochandlerx86

Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{a6b222ab-a5ea-4899-b230-

084657eddc7d}\localserver

Opens key: HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\localserver
Opens key: HKLM\software\microsoft\internet explorer\security\floppy access
Opens key: HKCU\software\microsoft\internet explorer\security\adv addrbar spoof

detection

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

detection

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

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

Opens key: HKCU\software\microsoft\internet explorer\zoom Opens key: HKLM\software\microsoft\internet explorer\zoom

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

Opens key: HKCU\software\microsoft\internet explorer\phishingfilter
Opens key: HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-

00aa00686f13}\progid

Opens key: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid Opens key: HKCU\software\microsoft\internet explorer\international

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

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

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

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

Opens key: HKCU\software\microsoft\windows\currentversion\policies
Opens key: HKCU\software\microsoft\internet explorer\pagesetup
Opens key: HKCU\software\microsoft\internet explorer\menuext
Opens key: HKCU\software\microsoft\internet explorer\menuext\%s
Opens key: HKLM\system\currentcontrol\nls\codepage

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

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

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

Opens key: HKCU\software\classes\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}

Opens key: HKCR\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}
Opens key: HKCU\software\classes\interface\{48a98a1f-5cdd-47ee-9286-

db04a3eb7ce1}\proxystubclsid32

Opens key: HKCR\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}\proxystubclsid32

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_zone_elevation Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_sslux Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_sslux HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_browser_emulation Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_browser_emulation Opens key: ${\it HKLM \backslash software \backslash microsoft \backslash internet \ explorer \backslash browsere mulation}$ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\user agent Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\ua tokens Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\pre platform Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent\pre platform HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\user agent\pre platform $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \label{lem:hklmsoftware} In the constraint of the$ Opens key: agent\post platform Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent\post platform HKCU\software\microsoft\windows\currentversion\internet Opens key: settings\5.0\user agent\post platform HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_xssfilter Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_xssfilter Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones Opens key: HKCU\software\classes\interface\{00020400-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32 Opens key: HKCR\interface\{00020400-0000-0000-c000-00000000046}\proxystubclsid32 HKCU\software\classes\clsid\{00020420-0000-0000-c000-00000000046} Opens key: Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046} Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}\treatas Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046}\treatas HKCU\software\classes\clsid\{00020420-0000-0000-c000-Opens kev: 000000000046}\inprocserver32 HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserver32 Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-Opens key: 00000000046}\inprocserverx86 HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserverx86 Opens key: Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}\localserver32 HKCR\clsid\{00020420-0000-0000-c000-00000000046}\localserver32 Opens key: Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-00000000046}\inprochandler32 Opens key: Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000- $000000000046 \} \verb|\inprochandlerx86| \\$ HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprochandlerx86 Opens key: Opens key: HKCU\software\classes\clsid\{00020420-0000-0000-c000-00000000046}\localserver Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046}\localserver Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39} HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39} Opens key: Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32 $HKCR \c1sid \end{absolute} In processor \c2 feas-11cf-a442-00a0c90a8f39 \end{absolute} in processor \c2 feas-11cf-a442-00a0c$ Opens key: Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserverx86

Opens key: Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserverx86

HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandlerx86

Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\localserver

Opens key: HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\localserver

Opens key: HKCU\software\classes\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}

Opens key: HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}
Opens key: HKCU\software\classes\interface\{d30c1661-cdaf-11d0-8a3e-

00c04fc9e26e}\proxystubclsid32

Opens key: HKCR\clsid\{00020424-0000-0000-0000000000046} Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-

000000000046}\treatas

00000000046}\inprocserver32

Opens key: HKCR\clsid\{00020424-0000-0000-c000-0000000046}\inprocserver32

Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-

00000000046}\inprocserverx86

Opens key: HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-

00000000046}\localserver32

Opens key: HKCR\clsid\{00020424-0000-0000-c000-00000000046}\localserver32

Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-

00000000046}\inprochandler32

Opens key: HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprochandler32

Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-

00000000046}\inprochandlerx86

Opens key: HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{00020424-0000-0000-c000-

00000000046}\localserver

Opens key: HKCR\clsid\{00020424-0000-0000-00000000000046}\localserver Opens key: HKCU\software\classes\interface\{d30c1661-cdaf-11d0-8a3e-

00c04fc9e26e}\forward

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

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

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

0000c05bae0b}\1.1\0

 $\label{lem:continuous} Opens~key: $$ HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0 $$ Opens~key: $$ HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-}$$

0000c05bae0b}\1.1\0\win32

Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32 Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}

Opens key: HKCR\typelib\{00020430-0000-0000-0000-00000000046}

Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-0000-00000000046}\2.0

Opens key: HKCR\typelib\{00020430-0000-0000-0000000000046}\2.0 Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-

000000000046}\2.0\0

Opens key: HKCR\typelib\{00020430-0000-0000-00000000000046}\2.0\0
Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-

00000000046}\2.0\0\win32

Opens key: HKCR\typelib\{00020430-0000-0000-000000000046}\2.0\0\win32
Opens key: HKCU\software\classes\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}

Opens key: HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}
Opens key: HKCU\software\classes\interface\{6d5140c1-7436-11ce-8034-

00aa006009fa}\proxystubclsid32

Opens key: $\label{eq:hkcr} \begin{tabular}{ll} HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32\\ Opens key: \\ HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\} \end{tabular}$

 Opens key:
 HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\

 Opens key:
 HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\

00a0c90dcaa9}\treatas

 $\label{lem:continuous} Opens key: $$ HKCR\clsid\b8da6310-e19b-11d0-933c-00a0c90dcaa9}\treatas $$ Opens key: $$ HKCU\software\classes\clsid\b8da6310-e19b-11d0-933c-$$$

00a0c90dcaa9}\inprocserver32

Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserver32

Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-

00a0c90dcaa9}\inprocserverx86

Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-

00a0c90dcaa9}\localserver32

Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\localserver32

Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-

00a0c90dcaa9}\inprochandler32

Opens key: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprochandler32

Opens key: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-

00a0c90dcaa9}\inprochandlerx86 HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprochandlerx86 Opens kev: HKCU\software\classes\clsid\{b8da6310-e19b-11d0-933c-Opens kev: 00a0c90dcaa9}\localserver Opens kev: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\localserver Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\actxprxy.dll HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85} Opens key: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85} Opens key: Opens key: HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32 $HKCR \verb|\interface| \{85cb6900-4d95-11cf-960c-0080c7f4ee85\} \verb|\proxystubclsid32|$ Opens key: Opens key: HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward Opens key: HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-Opens key: 0080c7f4ee85}\typelib HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert HKCU\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\ Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\ HKLM\software\microsoft\windows\currentversion\internet settings\ Opens key: Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ HKCU\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\ Opens key: HKCU\software\classes\interface\{9d973e3b-f610-4f03-83d3-aed90c3237ac} HKCR\interface\{9d973e3b-f610-4f03-83d3-aed90c3237ac} Opens key: Opens key: HKCU\software\classes\interface\{9d973e3b-f610-4f03-83d3aed90c3237ac}\synchronousinterface HKCR\interface\{9d973e3b-f610-4f03-83d3-Opens key: aed90c3237ac}\synchronousinterface HKCU\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_status_bar_throttling HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_status_bar_throttling $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8$ Opens key: c9633f71be64}\languageprofile\0x00000000 HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-Opens kev: c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d} Opens key: HKCU\software\policies\microsoft\internet explorer\control panel Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_urlecho Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_iedde_register_urlecho HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\ Opens key: Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105 Opens kev: HKLM\software\microsoft\internet explorer\activex compatibility Opens key: HKLM\software\microsoft\internet explorer\activex compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501} Opens key: HKCU\software\microsoft\windows\currentversion\ext\settings\{08b0e5c0-4fcb-11cf-aaa5-00401c608501} Opens key: $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{08b0e5c0-text\} = \{08b0e5$ 4fcb-11cf-aaa5-00401c608501} Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_alloweddomainlist HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_alloweddomainlist Opens key: HKLM\software\microsoft\internet explorer\extension compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501} HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_restrict_activexinstall Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_activexinstall Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{aaf8c6ce-f972-11d0-97eb-00aa00615333\}$ Opens key: HKCR\clsid\{aaf8c6ce-f972-11d0-97eb-00aa00615333} Opens key: HKCU\software\microsoft\code store database\distribution units Opens key: HKLM\software\microsoft\code store database\distribution units HKLM\software\microsoft\code store database\distribution Opens kev: units\{08b0e5c0-4fcb-11cf-aaa5-00401c608501} HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-Opens key:

Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\installedversion

HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\availableversion

HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-

00401c608501}\availableversion

00401c608501}\installedversion

Opens key: Opens key: Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\appid

Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\appid Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-

00401c608501}\inprocserver32

Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\inprocserver32

Opens key: HKCU\software\classes\clsid\{08b0e5c0-4fcb-11cf-aaa5-

00401c608501}\localserver32

Opens key: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\localserver32

Opens key: HKCU\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915| \\$

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_consult_mime_killbit_kb905915

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcbb}\treatas

Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\treatas
Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserver32

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcbb}\inprocserverx86

Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcbb}\localserver32

Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\localserver32

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcbb}\inprochandler32

Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprochandler32

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcbb}\inprochandlerx86

Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcbb}\localserver

Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}\localserver

Opens key: HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}

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

options\jp2iexp.dll

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547

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

options\wsock32.dll

Opens key: HKCU\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\feature_binary_caller_service_provider| \\$

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_binary_caller_service_provider

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

options\jvm.dll

Opens key: ${\tt HKCU \backslash software \backslash classes \backslash htmlfile \backslash shell}$

Opens key: HKCR\htmlfile\shell

Opens key: HKCU\software\classes\htmlfile\shell\opennew

Opens key: HKCR\htmlfile\shell\opennew

Opens key: HKCU\software\classes\htmlfile\shell\edit

Opens key: HKCR\htmlfile\shell\edit

Opens key: HKCU\software\classes\htmlfile\shell\edit\command

Opens key: HKCR\htmlfile\shell\edit\command

Opens key: ${\tt HKLM\backslash software\backslash microsoft\backslash internet\ explorer\backslash default\ html\ editor}$

Opens key: HKCU\software\classes\.html\openwithlist

Opens key: HKCR\.html\openwithlist

Opens key: $\begin{tabular}{ll} HKCU\software\microsoft\internet explorer\default html editor \\ Opens key: \\ HKLM\software\microsoft\internet explorer\default html editor \\ \end{tabular}$

 $Opens\;key: \\ \qquad \qquad \text{HKLM} software \\ \text{microsoft} internet\;explorer \\ \text{default}\;html\;editor \\ \text{shell} \\ \text{edit}$

Opens key: ${\tt HKLM\backslash software\backslash microsoft\backslash internet\ explorer\backslash default\ html}$

editor\shell\edit\command

Opens key: HKCU\software\microsoft\internet explorer\default mhtml editor
Opens key: HKLM\software\microsoft\internet explorer\default mhtml editor
Opens key: HKLM\software\microsoft\internet explorer\default mhtml

editor\shell\edit\command

 $Opens \ key: \\ HKCU \ software \ microsoft \ windows \ current version \ explorer \ fileexts \ . \ htm$

Opens key: HKCU\software\classes\.htm

Opens key: HKCR\.htm

Opens key: HKCU\software\classes\.htm\openwithlist

Opens key: HKCR\.htm\openwithlist

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

Opens key: HKCR\applications\notepad.exe

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

options\verify.dll

Opens key: HKCR\applications\notepad.exe\

Opens key: HKCU\software\classes\applications\notepad.exe\shell\edit

Opens key: HKCR\applications\notepad.exe\shell\edit

 $Opens~key: \\ HKCU \setminus software \land asses \land applications \land exe \land shell \land edit \land command \\$

```
Opens key: HKCR\applications\notepad.exe\shell\edit\command
```

Opens key: HKLM\software\policies\microsoft\internet explorer\feed discovery
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\java.dll

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

Opens key: HKCU\software\microsoft\ftp

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

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

Opens key: $\label{lem:hklmsoftware policies microsoft internet explorer activities} \\$

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

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

options\zip.dll

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\shell

Opens key: $\begin{tabular}{ll} HKCR\clsid\ff393560-c2a7-11cf-bff4-444553540000\shell\\ Opens key: \\ HKCU\software\classes\clsid\ff393560-c2a7-11cf-bff4- \end{tabular}$

444553540000}\shellex\iconhandler

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\clsid Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\inprocserver32

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\treatas

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\treatas Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\inprocserverx86

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\localserver32

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\localserver32

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\inprochandler32

Opens key: HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprochandler32

Opens key: HKCU\software\classes\clsid\{ff393560-c2a7-11cf-bff4-

444553540000}\inprochandlerx86

 $Opens~key: \\ HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\\\ \label{eq:c2a7-11cf-bff4-444553540000}\\\ \label{eq:c2a7-11cf-bff4-444553540000}$

Opens key: $\label{local-classeslik} \begin{tabular}{ll} HKCU \software \classes \clsid \ff 393560-c2a 7-11cf-bff 4-12cd-belle \classes \clsid \clsi$

444553540000}\localserver

 $Opens~key: \\ HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\label{localserver} \\ \\ Opens~key: \\ HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\label{localserver} \\ \\ Opens~key: \\$

Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{ff393560-c2a7-11cf-

bff4-444553540000}

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

settings\5.0\cache\extensible cache\mshist012016032920160330

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\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-

3aea-1069-a2d8-08002b30309d}

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

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

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

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

Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}

Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache\
Opens key: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}

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

Opens key: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-

11cf-aaa5-00401c608501}\iexplore

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

Opens key: HKCU\software\microsoft\internet explorer\caretbrowsing
Opens key: HKLM\software\microsoft\internet explorer\caretbrowsing
Opens key: HKLM\software\microsoft\internet explorer\migration

Opens key: HKCU\software\classes\http

Opens key: HKCR\http

Opens key: HKCU\software\classes\http\shell\open\ddeexec\ifexec

Opens key: HKCR\http\shell\open\ddeexec\ifexec

Opens key: HKCU\software\classes\https

Opens key: HKCR\https

Opens key: HKCU\software\classes\https\shell\open\ddeexec\ifexec

Opens key: HKCR\https\shell\open\ddeexec\ifexec

Opens key: HKCU\software\classes\ftp

Opens key: HKCR\ftp

Opens key: HKCU\software\classes\internetshortcut

Opens key: HKCR\internetshortcut

Opens key: HKCU\software\classes\internetshortcut\defaulticon

Opens key: HKCR\internetshortcut\defaulticon

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

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

Opens key: HKCU\software\classes\http\shell\open\ddeexec

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

Opens key: HKCU\software\classes\http\shell\open\ddeexec\application

Opens key: HKCR\http\shell\open\ddeexec\application

Opens key: HKCU\software\classes\http\shell\open\ddeexec\topic

Opens key: ${\tt HKCR\http\shell\open\ddeexec\topic}$

Opens key: HKCU\software\classes\https\shell\open\ddeexec

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

 $Opens~key: \\ HKCU \ software \ llopen \ deexec \ application$

Opens key: HKCR\https\shell\open\ddeexec\application

Opens key: HKCU\software\classes\https\shell\open\ddeexec\topic

Opens key: HKCR\https\shell\open\ddeexec\topic

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

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

Opens key: HKCU\software\classes\ftp\shell\open\ddeexec

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

Opens key: HKCU\software\classes\ftp\shell\open\ddeexec\ifexec

Opens key: HKCR\ftp\shell\open\ddeexec\ifexec

Opens key: HKCU\software\classes\ftp\shell\open\ddeexec\application

Opens key: HKCR\ftp\shell\open\ddeexec\application

Opens key: HKCU\software\classes\ftp\shell\open\ddeexec\topic

Opens key: HKCR\ftp\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\htmlfile\shell\open

Opens key: HKCR\htmlfile\shell\open

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

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

Opens key: HKCU\software\classes\htmlfile\shell\open\ddeexec

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

Opens key: HKCU\software\classes\htmlfile\shell\open\ddeexec\application

Opens key: ${\tt HKCR\htmlfile\shell\open\ddeexec\application}$

Opens key: HKCU\software\classes\htmlfile\shell\open\ddeexec\topic

Opens key: HKCR\htmlfile\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\mhtmlfile\shell

Opens key: HKCR\mhtmlfile\shell

 $Opens\;key: \\ \qquad \qquad \mathsf{HKCU} \\ \mathsf{Software} \\ \mathsf{classes} \\ \mathsf{htmlfile} \\ \mathsf{shell} \\ \mathsf{opennew} \\ \mathsf{command} \\$

Opens key: HKCR\htmlfile\shell\opennew\command

Opens key: HKCU\software\classes\htmlfile\shell\opennew\ddeexec

Opens key: HKCR\htmlfile\shell\opennew\ddeexec

Opens key: HKCU\software\classes\htmlfile\shell\opennew\ddeexec\ifexec

Opens key: ${\tt HKCR\htmlfile\shell\opennew\ddeexec\life} {\tt HKCR\htmlfile\shell\opennew\ddeexec\life}$

 $Opens\ key: \\ HKCU \ software \ classes \ htmlfile \ shell \ opennew \ dde exec \ application$

Opens key: HKCR\htmlfile\shell\opennew\ddeexec\application

Opens key: HKCU\software\classes\htmlfile\shell\opennew\ddeexec\topic

Opens key: HKCR\htmlfile\shell\opennew\ddeexec\topic

Opens key: HKCU\software\classes\.mht

Opens key: HKCR\.mht

Opens key: HKCU\software\classes\.mhtml

Opens key: HKCR\.mhtml

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

Opens key: HKCR\mhtmlfile\shell\open

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

Opens key: ${\tt HKCR\backslash mhtmlfile\backslash shell\backslash open\backslash command}$

 $Opens \; key: \\ \qquad \qquad \mathsf{HKCU} \\ \mathsf{software} \\ \mathsf{classes} \\ \mathsf{mhtmlfile} \\ \mathsf{shell} \\ \mathsf{open} \\ \mathsf{ddeexec} \\$

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

Opens key: HKCU\software\classes\mhtmlfile\shell\open\ddeexec\application

Opens key: ${\tt HKCR\mhtmlfile\shell\open\ddeexec\application}$

Opens key: HKCU\software\classes\mhtmlfile\shell\open\ddeexec\topic

Opens key: HKCR\mhtmlfile\shell\open\ddeexec\topic
Opens key: HKCU\software\classes\mhtmlfile\shell\opennew

Opens key: HKCR\mhtmlfile\shell\opennew

Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\command

Opens key: HKCR\mhtmlfile\shell\opennew\command

Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\ddeexec

Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec

Opens key: $\label{loopennew} \verb|HKCU| software\classes\m|htmlfile\shell\opennew|ddeexec\ifexec| } \\$

Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec\ifexec

Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\ddeexec\application

Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec\application

Opens key: HKCU\software\classes\mhtmlfile\shell\opennew\ddeexec\topic

Opens key: HKCR\mhtmlfile\shell\opennew\ddeexec\topic

Opens key: HKCU\software\classes\.url

Opens key: HKCR\.url

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

Opens key: HKCR\internetshortcut\clsid

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

Opens key: HKCR\internetshortcut\shell\open

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

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

Opens key: HKCU\software\classes\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837}

Opens key: HKCR\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837}

Opens key: HKCU\software\classes\applications\iexplore.exe\shell\open\command

Opens key: HKCR\applications\iexplore.exe\shell\open\command
Opens key: HKCU\software\microsoft\cryptography\providers\type 001

Opens key: HKLM\software\microsoft\cryptography\defaults\provider types\type 001
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider

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

options\rsaenh.dll

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

Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKCU\software\microsoft\internet explorer\user preferences

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

options\msasn1.dll

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

options\crypt32.dll

Opens key: HKLM\system\currentcontrolset\services\crypt32\performance
Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1

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

options\deploy.dll

Opens key: ${\tt HKLM} software \verb|microsoft| windows nt| current version \verb|limage file execution| }$

options\jp2native.dll

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

options\net.dll

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

options\nio.dll

Opens key: HKLM\software\oracle\javafx

Opens key: HKLM\software\javasoft\java runtime environment\1.7

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

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

Opens key: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\appcompatflags\custom\java.exe|$

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

options\java.exe

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

options\shimeng.dll

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

options\awt.dll

Opens key: ${\tt HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus java.exe}$

Opens key: HKLM\hardware\devicemap\video

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

options\d3d8thk.dll

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

options\d3d9.dll

Opens key: HKLM\software\microsoft\direct3d

 $Opens~key: \\ HKLM\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-40$

9b1f4867732a}\0000

Opens key: HKLM\software\microsoft\direct3d\drivers

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

options\java.exe\rpcthreadpoolthrottle

Opens key: HKLM\software\javasoft\java update\policy

 $Opens\ key: \\ HKCU \ software \ microsoft \ windows \ current version \ policies \ comdlg 32 \\$

Opens key:

 $HKCU \ software \ microsoft \ windows \ current version \ policies \ comdlg 32 \ places bar \ not the combination \ policies \ not the combination \ policies \ not the combination \ not the combin$

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

options\fontmanager.dll

Opens key: HKCU\eudc\1252

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

options\t2k.dll

Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-

c9633f71be64}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}

Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-

77e8f3d1aa80}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}

Opens key: HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-

Opens key: $\label{logo} HKLM \software\microsoft\tip\f89e9e58 of 816c09f4ee} \category\tem\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}$

HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Queries value: $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles] HKLM\software\microsoft\windows Oueries value: nt\currentversion\compatibility32[iexplore] HKLM\software\microsoft\windows nt\currentversion\ime Queries value: compatibility[iexplore] Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]

Oueries value: HKLM\system\setup[systemsetupinprogress] HKCU\control panel\desktop[multiuilanguageid] Oueries value: Queries value: HKCU\control panel\desktop[smoothscroll] Oueries value:

 $\label{thm:local_equation} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced[enableballoontips] \end{tabular}$

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

manager[criticalsectiontimeout]

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

Queries value: HKCR\interface[interfacehelperdisableall]

Queries value: HKCR\interface[interfacehelperdisableallforole32] HKCR\interface[interfacehelperdisabletypelib] Oueries value: Queries value: HKCR\interface\{00020400-0000-0000-c000-

00000000046}[interfacehelperdisableall]

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

00000000046}[interfacehelperdisableallforole32]

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

settings[disableimprovedzonecheck]

HKLM\software\microsoft\internet Queries value:

explorer\main\featurecontrol\feature_protocol_lockdown[iexplore.exe]

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

ab78-1084642581fb]

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

0000-0000000000001

Queries value: HKLM\software\microsoft\internet explorer\main[depoff]

HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[] Oueries value: $\label{lem:hklm} \verb+Kklm/software/microsoft/internet explorer/setup[iexplorelastmodifiedlow]+ \\$ Oueries value:

HKLM\software\microsoft\internet Queries value:

explorer\setup[iexplorelastmodifiedhigh]

Queries value:

manager[safeprocesssearchmode]

HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[] Oueries value: HKLM\software\microsoft\internet explorer\setup[installstarted] Oueries value:

Oueries value: Queries value: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[] HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[] Oueries value: Queries value: $HKCR \ interface \ \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\} \ proxystubclsid32[]$

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

settings[fromcachetimeout]

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

settings[secureprotocols]

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

explorer\main[security_hklm_only]

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

settings[certificaterevocation]

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

settings[disablekeepalive]

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

settings[disablepassport]

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

Queries value:

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

Queries value:

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ settings[enablehttp1_1]

Queries value:

HKCU\software\microsoft\windows\currentversion\internet

settings[proxyhttp1.1]

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

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

settings[disablebasicoverclearchannel]

HKCU\software\microsoft\internet Oueries value: explorer\main\featurecontrol[feature_clientauthcertfilter] Queries value: HKLM\software\microsoft\internet 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]

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

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

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

```
settings\5.0\cache[signature]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\content[peruseritem]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\content[cacheprefix]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[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\cookies[peruseritem]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries 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]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\cookies[cachelimit]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[history]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[cachelimit]
                           HKLM\software\microsoft\rpc[maxrpcsize]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
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:
                           \label{lem:hkcu} \verb+KCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings\5.0\cache\extensible cache\feedplat[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ 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]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacherepair]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                           \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
```

```
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries 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]
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxhttpredirects]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                            \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
 Queries value:
settings[maxconnectionsperserver]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
                            \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
 Queries value:
settings[maxconnectionsper1 Oserver]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[serverinfotimeout]
 Queries value:
                            \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[connecttimeout]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                            \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Oueries value:
settings[disablentlmpreauth]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelifetime]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[httpdefaultexpirytimesecs]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
 Queries value:
                            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[iexplore.exe]
                            HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
```

```
Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[leashlegacycookies]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablent4rascheck]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dialupuselansettings]
                            HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dialupuselansettings]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[sendextracrlf]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypassftptimecheck]
                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[releasesocketduringauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[releasesocketduring401auth]
                            HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[releasesocketduring401auth]
  Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablelegacypreauthasserver]
                            HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablelegacypreauthasserver]
  Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[enablehttptrace]
                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
  Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
  Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
  Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscacheentries]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnalwaysonpost]
  Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[warnonzonecrossing]
  Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[warnonbadcertsending]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonbadcertrecving]
  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[warnonpostredirect]
  Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[alwaysdrainonredirect]
                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonhttpstohttpredirect]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
```

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 000000000001 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled] Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000002 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000003 [supported namespace] \\ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
 Oueries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 spin count]$
- Oueries value: HKCU\software\microsoft\windows\currentversion\internet
- settings[globaluseroffline]
- Queries value: HKCU\software\microsoft\windows\currentversion\internet
- settings[enableautodial]
- Queries value: HKLM\software\microsoft\windows\currentversion\internet
- settings[urlencoding]

```
Queries value:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
   Queries value:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[migrateproxy]
   Queries value:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
   Queries value:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[proxyoverride]
   Queries value:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\connections[savedlegacysettings]
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\connections[defaultconnectionsettings]
   Queries value:
                                                         HKCU\software\microsoft\internet explorer\main[start page]
   Oueries value:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
                                                         HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[createuricachesize]
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[enablepunycode]
                                                         HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[enablepunycode]
                                                         HKCU\software\microsoft\internet explorer\main[secondary start pages]
   Queries value:
   Oueries value:
                                                         HKLM\software\microsoft\internet explorer\main[secondary start pages]
   Queries value:
                                                         HKCU\software\microsoft\internet explorer\main[frametabwindow]
   Queries value:
                                                         HKLM\software\microsoft\internet explorer\main[frametabwindow]
                                                         \label{lem:hkcu} \verb+KKCU\+ software \verb+\microsoft\+ internet explorer \verb+\main[framemerging]
   Queries value:
                                                         HKLM\software\microsoft\internet explorer\main[framemerging]
   Queries value:
   Queries value:
                                                         HKCU\software\microsoft\internet explorer\main[sessionmerging]
   Oueries value:
                                                         HKLM\software\microsoft\internet explorer\main[sessionmerging]
                                                         HKCU\software\microsoft\internet explorer\main[admintabprocs]
   Queries value:
                                                         HKLM\software\microsoft\internet explorer\main[admintabprocs]
   Oueries value:
                                                         HKLM \setminus software \setminus policies \setminus microsoft \setminus internet \ explorer \setminus main[tabprocgrowth]
   Oueries value:
                                                         HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
   Queries value:
   Queries value:
                                                         HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
   Oueries value:
                                                         HKCU\software\microsoft\internet explorer\main[hangresistantframe]
                                                         HKLM\software\microsoft\internet explorer\main[hangresistantframe]
   Queries value:
                                                         HKCU\software\microsoft\internet explorer\main[compatibilityflags]
   Oueries value:
   Oueries value:
                                                         HKCU\software\microsoft\internet explorer\new windows[detourdialogs]
                                                         HKLM\software\microsoft\ctf\systemshared[cuas]
   Oueries value:
                                                         HKCU\keyboard layout\toggle[language hotkey]
   Queries value:
   Oueries value:
                                                         HKCU\keyboard layout\toggle[hotkey]
                                                         HKCU\keyboard layout\toggle[layout hotkey]
   Queries value:
   Oueries value:
                                                         HKLM\software\microsoft\ctf[enableanchorcontext]
                                                         \label{locations} \verb|HKLM\software\microsoft\ole[maximum allowed allocation size]| \\
   Queries value:
                                                         HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
   Oueries value:
   Oueries value:
                                                         HKCU\software\microsoft\internet explorer\sqm[serverfreezeonuploadl]
   Queries value:
                                                         HKLM\software\microsoft\internet explorer\sqm[serverfreezeonupload]
   Queries value:
                                                         HKLM\software\microsoft\windows\currentversion[programfilesdir]
                                                         HKCU\software\microsoft\internet
   Oueries value:
explorer\sqm[disablecustomerimprovementprogram]
   Oueries value:
                                                         HKLM\software\microsoft\internet
explorer\sqm[disablecustomerimprovementprogram]
                                                         HKCU\software\microsoft\internet explorer\sqm[sqmoptinforie8]
   Oueries value:
                                                         HKLM\software\microsoft\internet explorer\sqm[sqmoptinforie8]
   Queries value:
   Queries value:
                                                         HKCU\software\microsoft\internet
explorer\browseremulation[unattendloaded]
                                                         HKCU\software\microsoft\internet explorer\browseremulation[tldupdates]
   Queries value:
                                                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Oueries value:
folders[desktop]
                                                         HKCU \ software \ microsoft \ windows \ current version \ ext \ settings \ \{18df081c-microsoft\} \ description \ ext \ description \ descript
   Oueries value:
e8ad-4283-a596-fa578c2ebdc3}[flags]
                                                         HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}\inprocserver32[]
   Oueries value:
   Queries value:
                                                         HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus windows \setminus current version \setminus ext \setminus settings \setminus \{18df081c-microsoft \setminus ext \setminus
e8ad-4283-a596-fa578c2ebdc3}[vercache]
   Queries value:
                                                         HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-
a445-435b-bc74-9c25c1c588a9}[flags]
                                                         HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}\inprocserver32[1
   Oueries value:
   Oueries value:
                                                         HKCU\software\microsoft\windows\currentversion\ext\settings\{dbc80044-
a445-435b-bc74-9c25c1c588a9}[vercache]
   Oueries value:
                                                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
   Oueries value:
                                                         HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
   Oueries value:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
                                                         HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\1[flags]
```

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2[flags] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[flags] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\4[flags] Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_localmachine_lockdown[iexplore.exe] Queries value: HKLM\software\policies\microsoft\internet explorer\security[disablefixsecuritysettings] HKCU\software\microsoft\internet Oueries value: explorer\security[disablefixsecuritysettings] HKLM\software\microsoft\internet Queries value: explorer\security[disablefixsecuritysettings] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[] HKLM\system\wpa\pnp[seed] Queries value: HKLM\system\setup[osloaderpath] Oueries value: HKLM\system\setup[systempartition] Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath] Queries value: HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath] HKLM\software\microsoft\windows\currentversion\setup[drivercachepath] Queries value: HKLM\software\microsoft\windows\currentversion[devicepath] Oueries value: Oueries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel] HKLM\software\microsoft\windows\currentversion\setup[logpath] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[data] 11e3-9fc7-806d6172696f}[generation] Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden] HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Oueries value: Queries value: Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview] Oueries value: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \policies \explorer[classicshell] \end{tabular}$ Queries value: $HKCU \ software \ microsoft \ windows \ current version \ policies \ explorer [separate process]$ HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu] HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Queries value: Oueries value: Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Oueries 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] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Queries value: Queries value: HKCR\directory[docobject] Oueries value: HKCR\directory[browseinplace] HKCR\directory[isshortcut] Oueries value: Queries value: HKCR\directory[alwaysshowext] Oueries value: HKCR\directory[nevershowext] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions] HKCU\software\microsoft\windows\currentversion\explorer\user shell Queries value: folders[recent] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html[progid] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html[application] Queries value: HKCR\.html[] Oueries value: HKCR\htmlfile\shellex\iconhandler[] Queries value: HKCR\htmlfile[docobject] Queries value: HKCR\.html[perceivedtype] HKCR\systemfileassociations\text[docobject] Oueries value: Queries value: HKCR\htmlfile[browseinplace] Queries value: HKCR\systemfileassociations\text[browseinplace] HKCR\htmlfile\clsid[] Queries value: HKCR\htmlfile[isshortcut] Queries value: Queries value: HKCR\systemfileassociations\text[isshortcut] Oueries value: HKCR\htmlfile[alwaysshowext] HKCR\systemfileassociations\text[alwaysshowext] Queries value: Oueries value: HKCR\htmlfile[nevershowext] Queries value: HKCR\systemfileassociations\text[nevershowext] manager\appcompatibility[disableappcompat] Oueries value: $\label{lem:hklmsoftware policies microsoft windows safer code identifiers [authenticode enabled] \\$ HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels] Oueries value: Oueries value: be2efd2c1a33}[itemdata] Queries value: be2efd2c1a33}[saferflags] Queries value: edd5fbde1328}[itemdata] Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[hashalg] Queries value: edd5fbde1328}[itemsize] Queries value: edd5fbde1328}[saferflags] Queries value: b813f72dbb91}[itemdata] Oueries value: b813f72dbb91}[hashalg] Oueries value:

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

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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-

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

Queries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{7fb9cd2e-3076-4df9-a57b-4df9-a57$ b813f72dbb91}[saferflags]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{94e3e076-8f53-42a5-8411-14414 \setminus 1449-14414 \setminus 1449-1440-14414 + 1449-1440-1440 + 1449-1440 + 1449-1440-1440 + 1449-1440-1440 + 1449-1440-1440 + 14$ 085bcc18a68d}[itemdata]

Queries value:

```
085bcc18a68d}[hashalg]
 Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[saferflags]
 Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
 Queries value:
b91490411bfc}[hashalg]
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
 Queries value:
b91490411bfc [saferflags]
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
 Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
                        HKCU\software\microsoft\windows\currentversion\explorer\shell
 Queries value:
folders[cache]
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
 Queries value:
 Queries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
 Queries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
 Queries value:
 Queries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
 Queries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
 Oueries value:
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
 Queries value:
 Queries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
 Oueries value:
                        HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi2]
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
 Queries value:
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
 Queries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
 Oueries value:
                        HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi8]
 Queries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
 Oueries 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]
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
 Queries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
 Queries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
 Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
 Queries value:
 Oueries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
 Queries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
 Queries value:
                        HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer31
 Oueries value:
```

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]

Queries value:

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus telephony [tapi32 max numre questre tries]$

Queries value:

Queries value: HKLM\software\microsoft\tracing\rasapi32[filetracingmask]

Queries value: HKLM\software\microsoft\tracing\rasapi32[enabletracingmask]

Queries value: HKLM\software\microsoft\tracing\rasapi32[consoletracing]

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\currentcontrol\set\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[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\internet explorer\main[window_min_width]
Queries value: HKCU\software\microsoft\internet explorer\main[window_min_height]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKCU\software\microsoft\internet explorer\recovery[enabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[local appdata]

Queries value: HKLM\software\microsoft\com3[gipactivitybypass]

Queries value: HKCR\interface\{1ac7516e-e6bb-4a69-b63f-e841904dc5a6}\proxystubclsid32[]

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

Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]

Queries value: HKLM\software\microsoft\com3[regdbversion]
Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-

e4fddd701cba}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]

Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[appid]

Queries value: HKCR\clsid\{a4a1a128-768f-41e0-bf75-

e4fddd701cba}\inprocserver32[threadingmodel]

Queries value: HKCR\interface\{7673b35e-907a-449d-a49f-e5ce47f0b0b2}\proxystubclsid32[]

 $\label{thm:condition} Queries \ value: \\ HKCU \ software \ microsoft \ internet \ explorer \ tabbed browsing [groups]$

Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-

f4ceaaf59cfc}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]

Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid]

Queries value: HKCR\clsid\{50d5107a-d278-4871-8989-

f4ceaaf59cfc}\inprocserver32[threadingmodel]

 $\label{lem:queries value: HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}\[enable]$

Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-

431b3828ba53}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]

Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid]

Queries value: HKCR\clsid\{3ce74de4-53d3-4d74-8b83-

431b3828ba53}\inprocserver32[threadingmodel]

Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[]

Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]

Queries value: HKCR\clsid\{a4b544a1-438d-4b41-9325-

869523e2d6c7}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[description]
Queries value: HKLM\software\policies\microsoft\internet

explorer\main[tabshutdowndelay]

Queries value: HKCU\software\microsoft\internet explorer\main[tabshutdowndelay]
Queries value: HKLM\software\microsoft\internet explorer\main[tabshutdowndelay]

Queries value: HKCU\software\microsoft\internet

 ${\tt explorer} \verb|\main| windows search[enabled scopes]|$

Queries value: HKCR\.url\persistenthandler[]

Queries value: HKLM\software\microsoft\windows search[currentversion]

Queries value: HKCU\software\microsoft\internet explorer\main[window_placement]

Queries value: HKCU\software\microsoft\internet

explorer\toolbar\webbrowser[itbar7position]

```
HKCU\software\microsoft\internet explorer\main[fullscreen]
      Oueries value:
                                                                                        \label{thm:linear} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| the memanager [compositing] \end{tabular}
      Oueries value:
      Oueries value:
                                                                                        HKCU\control panel\desktop[lamebuttontext]
                                                                                        HKLM\software\microsoft\windows\currentversion\explorer[max cached
      Queries value:
 icons1
      Queries value:
                                                                                        HKCU\control panel\desktop\windowmetrics[shell icon size]
                                                                                        HKCU\control panel\desktop\windowmetrics[shell small icon size]
      Queries value:
      Oueries value:
                                                                                        HKCU\control panel\desktop\windowmetrics[shell icon bpp]
      Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers\offline
files[suppressionpolicy]
      Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers\offline
files[]
      Queries value:
                                                                                        HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserver32[]
      Queries value:
                                                                                       HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprocserver32[loadwithoutcom]
      Queries value:
                                                                                       HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-
 080036587f03}\inprocserver32[inprocserver32]
                                                                                       HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}[appid]
      Queries value:
      Queries value:
                                                                                       HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprocserver32[threadingmodel]
                                                                                      HKCR\clsid\{b5f8350b-0548-48b1-a6ee-
      Oueries value:
 88bd00b4a5e7}\inprocserver32[inprocserver32]
      Queries value:
                                                                                       HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}\inprocserver32[]
      Oueries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [used esktopinicache]
                                                                                       HKCR\clsid\{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}[appid]
      Queries value:
                                                                                       HKCR\clsid\{b5f8350b-0548-48b1-a6ee-
      Oueries value:
 88bd00b4a5e7}\inprocserver32[threadingmodel]
      Queries value:
                                                                                       HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1[]
                                                                                        HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\flags[]
      Queries value:
      Queries value:
                                                                                        HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0\win32[]
      Queries value:
                                                                                        HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}[]
                                                                                        HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\proxystubclsid[]
      Oueries value:
      Queries value:
                                                                                        Queries value:
                                                                                        HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\typelib[]
                                                                                        HKCR\interface\{618736e0-3c3d-11cf-810c-00aa00389b71}\typelib[version]
      Oueries value:
                                                                                        HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}[]
      Queries value:
      Queries value:
                                                                                        HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\proxystubclsid[]
                                                                                        HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\proxystubclsid32[]
      Oueries value:
                                                                                        HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\typelib[]
      Queries value:
                                                                                        HKCR\interface\{03022430-abc4-11d0-bde2-00aa001a1953}\typelib[version]
      Oueries value:
      Oueries value:
                                                                                        HKCU\software\microsoft\internet explorer\main[useie7autocomplete]
                                                                                        HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
      Oueries value:
                                                                                        HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
      Queries value:
      Queries value:
                                                                                       HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
                                                                                       HKCU\software\microsoft\internet explorer\main[searchcontrolwidth]
      Oueries value:
      Queries value:
                                                                                       HKCU\software\microsoft\internet explorer\main[searchmigrated]
                                                                                        HKCU\software\microsoft\internet explorer\main[searchmigratedinstalled]
      Oueries value:
                                                                                       HKCU\software\microsoft\internet
      Oueries value:
explorer\main[searchmigrateddefaultname]
                                                                                        HKCU\software\microsoft\internet explorer\main[searchmigrateddefaulturl]
      Queries value:
      Oueries value:
                                                                                        HKCU\software\microsoft\internet explorer\searchurl[provider]
      Queries value:
                                                                                        HKCU\software\microsoft\internet explorer\searchscopes[defaultscope]
                                                                                        HKCU \setminus software \setminus microsoft \setminus internet explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus microsoft \setminus microso
      Queries value:
472f-a0ff-e1416b8b2e3a}[deleted]
                                                                                       HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
      Oueries value:
472f-a0ff-e1416b8b2e3a}[url]
     Queries value:
                                                                                       HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus internet \ explorer \setminus search scopes \setminus search sc
472f-a0ff-e1416b8b2e3a}[displayname]
                                                                                        HKLM \setminus software \setminus microsoft \setminus internet explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus microsoft \setminus microso
      Queries value:
472f-a0ff-e1416b8b2e3a}[displayname]
                                                                                       Oueries value:
472f-a0ff-e1416b8b2e3a}[showsearchsuggestions]
     Queries value:
                                                                                       HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[showsearchsuggestions]
      Queries value:
                                                                                       HKCU\software\microsoft\internet
explorer\searchscopes[showsearchsuggestionsglobal]
      Queries value:
                                                                                       HKLM\software\microsoft\internet
 explorer\searchscopes[showsearchsuggestionsglobal]
      Oueries value:
                                                                                       HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[suggestionsurl_json]
      Queries value:
                                                                                       HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[suggestionsurl_json]
      Queries value:
                                                                                       HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[suggestionsurl_jsonfallback]
                                                                                       HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
     Oueries value:
472f-a0ff-e1416b8b2e3a}[suggestionsurl_jsonfallback]
      Queries value:
                                                                                       HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[suggestionsurl]
      Queries value:
                                                                                        HKLM \setminus software \setminus microsoft \setminus internet explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus microsoft \setminus microso
```

```
472f-a0ff-e1416b8b2e3a}[suggestionsurl]
                                                           HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
    Oueries value:
472f-a0ff-e1416b8b2e3a}[suggestionsurlfallback]
    Queries value:
                                                           HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[previewurl]
    Queries value:
                                                           HKLM \setminus software \setminus microsoft \setminus internet explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus microsoft \setminus microso
472f-a0ff-e1416b8b2e3a}[previewurl]
    Oueries value:
                                                           HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[previewurlfallback]
    Oueries value:
                                                           HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[previewurlfallback]
                                                           HKCU \setminus software \setminus microsoft \setminus internet explorer \setminus search scopes \setminus \{0633ee93-d776-microsoft \setminus microsoft \setminus microso
    Queries value:
472f-a0ff-e1416b8b2e3a}[faviconurl]
    Oueries value:
                                                           HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[faviconurl]
    Queries value:
                                                           HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
472f-a0ff-e1416b8b2e3a}[faviconurlfallback]
                                                           HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
    Queries value:
472f-a0ff-e1416b8b2e3a}[faviconpath]
                                                           HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
    Queries value:
472f-a0ff-e1416b8b2e3a}[codepage]
                                                           HKLM\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
    Queries value:
472f-a0ff-e1416b8b2e3a}[codepage]
                                                           HKCU\software\microsoft\internet explorer\searchscopes\{0633ee93-d776-
    Queries value:
472f-a0ff-e1416b8b2e3a}[sortindex]
                                                           HKCU\software\microsoft\internet explorer\tabbedbrowsing[enabled]
    Queries value:
                                                           HKCU\software\microsoft\internet explorer\toolbar[locked]
    Queries value:
                                                           HKCU\software\microsoft\internet explorer\linksbar[enabled]
    Queries value:
    Oueries value:
                                                           HKCU\software\microsoft\internet
explorer\tabbedbrowsing[activitymetertimerinterval]
                                                           HKCU\software\microsoft\internet
    Oueries value:
explorer\tabbedbrowsing[activitymeterdisable]
                                                           HKCU\software\microsoft\internet
    Queries value:
explorer\tabbedbrowsing[quicktabsthreshold]
    Oueries value:
                                                           HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-
4134-82b7-f2ba38496583}[clsid]
    Oueries value:
                                                           HKCU\software\microsoft\windows\currentversion\ext\stats\{e2e2dd38-d088-
4134-82b7-f2ba38496583}\iexplore[count]
                                                           Queries value:
4134-82b7-f2ba38496583}[buttontext]
    Queries value:
                                                           4134-82b7-f2ba38496583}[menutext]
                                                           HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-
   Oueries value:
4134-82b7-f2ba38496583}[menucustomize]
    Oueries value:
                                                           HKLM\software\microsoft\internet explorer\extensions\{e2e2dd38-d088-
4134-82b7-f2ba38496583}[menustatusbar]
    Queries value:
                                                           HKCU\software\microsoft\internet
explorer\lowregistry\extensions\cmdmapping[{e2e2dd38-d088-4134-82b7-f2ba38496583}]
                                                           HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
    Oueries value:
11d2-bb9e-00c04f795683}[clsid]
    Oueries value:
                                                           11d2-bb9e-00c04f795683}\iexplore[count]
    Queries value:
                                                           HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
11d2-bb9e-00c04f795683}[buttontext]
                                                           HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
   Oueries value:
11d2-bb9e-00c04f795683}[menutext]
    Queries value:
                                                           HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
11d2-bb9e-00c04f795683}[menucustomize]
    Oueries value:
                                                           HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
11d2-bb9e-00c04f795683}[menustatusbar]
                                                          HKCU\software\microsoft\internet
    Queries value:
explorer\lowregistry\extensions\cmdmapping[{fb5f1910-f110-11d2-bb9e-00c04f795683}]
                                                           Queries value:
11d2-bb9e-00c04f795683}[default visible]
    Oueries value:
                                                           HKLM\software\microsoft\internet explorer\extensions\{fb5f1910-f110-
11d2-bb9e-00c04f795683}[icon]
                                                           HKCU\software\microsoft\internet
    Queries value:
explorer\tabbedbrowsing[thumbnailbehavior]
    Queries value:
                                                          HKCU\software\microsoft\internet
explorer\toolbar\webbrowser[itbar7height]
                                                           HKCR\clsid\{0002df01-0000-0000-c000-
    Queries value:
000000000046}\localserver32[localserver32]
                                                           HKCR\clsid\{0002df01-0000-0000-c000-00000000046}\localserver32[]
    Oueries value:
    Oueries value:
                                                           HKCR\clsid\{d5e8041d-920f-45e9-b8fb-
b1deb82c6e5e}\localserver32[localserver32]
                                                           HKCR\clsid\{d5e8041d-920f-45e9-b8fb-b1deb82c6e5e}\localserver32[]
    Oueries value:
    Queries value:
                                                           HKLM\software\microsoft\rpc\securityservice[10]
    Oueries value:
HKLM \setminus system \setminus current control \setminus security providers [security providers]
    Oueries value:
                                                           HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
    Queries value:
Queries value:
```

```
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
   Oueries value:
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
   Oueries value:
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
   Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
   Oueries value:
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
   Oueries value:
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
   Queries value:
   Oueries value:
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
   Oueries value:
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
                                               HKLM\svstem\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
   Oueries value:
   Queries value:
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
   Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
   Queries value:
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
   Queries value:
                                               Oueries value:
   Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
                                               {\tt HKLM \setminus software \setminus microsoft \setminus rpc \setminus security service [default authlevel]}
   Queries value:
   Queries value:
                                               HKCU\software\microsoft\windows\currentversion\internet settings\url
history[daystokeep]
   Oueries value:
                                               HKCR\interface\{8a7476f4-d264-4e13-ae72-20cd9831d98c}\proxystubclsid32[]
   Queries value:
                                               HKCR \cdot face \{b40c43f1-f039-44d2-aeb7-87f5af8abc3d\} \cdot face \{b40c45f1-f039-44d2-aeb7-87f5af8abc3d\} \cdot face \{b40c45f1-f0366-aeb7-67f6af8abc3d\} \cdot face \{b40c45f1-f0366-aeb7-67f6af8abc3d\} \cdot face \{b40c45f1-f0366-
   Queries value:
                                               HKCR\interface\{d358f4e1-0465-4965-9dd5-cae303d2c345}\proxystubclsid32[]
                                               HKCR\interface\{ff18630e-5b18-4a07-8a75-9fd3ce5a2d14}\proxystubclsid32[]
   Queries value:
   Queries value:
                                               HKCU\software\microsoft\internet explorer\main[enableprebinding]
   Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| policies \verb|\explorer[nofilemenu]| \\
   Queries value:
                                               HKCU\software\microsoft\internet explorer\main[window title]
   Queries value:
                                               HKLM\software\policies\microsoft\internet explorer\main[statusbarweb]
                                               HKCU\software\microsoft\internet explorer\main[statusbarweb]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\internet explorer\main[statusbarweb]
   Queries value:
                                               HKLM\software\policies\microsoft\internet explorer\main[enable browser
extensions1
   Queries value:
                                               HKCU\software\microsoft\internet explorer\main[enable browser
extensions1
                                               HKLM\software\policies\microsoft\internet explorer\main[alwaysshowmenus]
   Queries value:
   Oueries value:
\label{thm:cursoft} $$ HKCU \software \microsoft \windows \current version \policies \explorer [noband customize] $$ is a substitution of the context of t
   Queries value:
                                               HKCU\software\microsoft\internet
explorer\toolbar\webbrowser[itbar7layout]
                                               HKCU\software\microsoft\internet explorer\main[alwaysshowmenus]
   Oueries value:
   Oueries value:
                                               HKLM\software\microsoft\internet explorer\main[alwaysshowmenus]
                                               HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
   Oueries value:
4283-a596-fa578c2ebdc3}\iexplore[count]
                                               HKCR\clsid\{18df081c-e8ad-4283-a596-
   Queries value:
fa578c2ebdc3}\inprocserver32[inprocserver32]
   Oueries value:
                                               HKCR\clsid\{18df081c-e8ad-4283-a596-fa578c2ebdc3}[appid]
                                               HKCR\appid\{77ab4812-5411-4ea9-8437-77ad0f230302}[dllsurrogate]
   Queries value:
                                               HKCR\appid\{77ab4812-5411-4ea9-8437-77ad0f230302}[localservice]
   Queries value:
   Queries value:
                                               HKCR\clsid\{18df081c-e8ad-4283-a596-
fa578c2ebdc3}\inprocserver32[threadingmodel]
                                               HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}\inprocserver32[]
   Queries value:
   Queries value:
                                               HKCR\clsid\{06849e9f-c8d7-4d59-b87d-
784b7d6be0b3}\inprocserver32[inprocserver32]
                                               HKCR\clsid\{06849e9f-c8d7-4d59-b87d-784b7d6be0b3}[appid]
   Queries value:
   Queries value:
                                               HKCR\clsid\{06849e9f-c8d7-4d59-b87d-
784b7d6be0b3}\inprocserver32[threadingmodel]
                                               HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-
   Oueries value:
4283-a596-fa578c2ebdc3}\iexplore[loadtimecount]
                                               Queries value:
4283-a596-fa578c2ebdc3}\iexplore[loadtime]
                                               HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-
   Oueries value:
435b-bc74-9c25c1c588a9}\iexplore[count]
                                              HKCR\clsid\{dbc80044-a445-435b-bc74-
9c25c1c588a9}\inprocserver32[inprocserver32]
                                              HKCR\clsid\{dbc80044-a445-435b-bc74-9c25c1c588a9}[appid]
   Queries value:
   Queries value:
                                              HKCR\clsid\{dbc80044-a445-435b-bc74-
9c25c1c588a9}\inprocserver32[threadingmodel]
                                               HKLM\software\javasoft\java plug-in\10.2.0[usenewjavaplugin]
   Queries value:
```

Queries value: HKLM\software\javasoft\java plug-in\10.2.0[usenewjavaplugin]
Queries value: HKLM\software\javasoft\java runtime environment\1.7.0_02[javahome]
Queries value: HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}\treatas[]
Queries value: HKCU\software\microsoft\internet explorer\suggested sites[enabled]
Queries value: HKCR\typelib\{5f226421-415d-408d-9a09-0dcd94e25b48}\1.0\0\win32[]
Queries value: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c00c04fb6bfc4}\inprocserver32[inprocserver32]

 $HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\tinprocserver32[]$ Oueries value: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}[appid] Oueries value: Oueries value: HKCR\clsid\{7b8a2d95-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[threadingmodel] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[icon] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[minlevel] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0[recommendedlevel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\0[currentlevel] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\1[icon] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\zones\1[minlevel] HKI M\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\1[recommendedlevel] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\1[currentlevel] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\2[icon] HKLM\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\2[minlevel] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings\zones\2[recommendedlevel] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\2[currentlevel] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[icon] HKLM\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\3[minlevel] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings\zones\3[recommendedlevel] $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}$ Queries value: settings\zones\3[currentlevel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\4[icon] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings\zones\4[minlevel] $\label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet$ Queries value: settings\zones\4[recommendedlevel] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\zones\4[currentlevel] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\ratings[kev] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[urlencoding] $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft + windows \verb+current version \verb+\internet+ in the lemma + the lemma$ Queries value: settings[specialfolderscachesize] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[specialfolderscachesize] HKCR\protocols\handler\about[clsid] Oueries value: Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[inprocserver32] HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[] Oueries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid] Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-Oueries value: 00aa00bdce0b}\inprocserver32[threadingmodel] Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_dispparams[iexplore.exe] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_legacy_dispparams[*] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature object caching[iexplore.exe] HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay] Queries value: HKLM\software\microsoft\internet explorer\application Oueries value:

compatibility[iexplore.exe]

HKCU\software\microsoft\internet explorer\domstorage[totallimit] Queries value: Queries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit]

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

explorer\main\featurecontrol\feature_mime_handling[iexplore.exe] Queries value: HKCR\.html[content type]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_sniffing[iexplore.exe]

Queries value: $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}$ settings\zones\3[2100]

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

settings[istextplainhonored]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_safe_bindtoobject[iexplore.exe]

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

```
00aa00686f13}\inprocserver32[inprocserver32]
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
 Oueries value:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid]
 Oueries value:
 Queries value:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[threadingmodel]
 Queries value:
                         HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinset]
                         HKCU\software\microsoft\windows
 Oueries value:
nt\currentversion\windows[dragscrolldelay]
 Oueries value:
                         HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload[iexplore.exe]
                        HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_restrict_filedownload[*]
 Queries value:
                         HKCR\clsid\{a6b222ab-a5ea-4899-b230-
084657eddc7d}\inprocserver32[inprocserver32]
                         HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}\inprocserver32[]
 Queries value:
 Oueries value:
                         HKCR\clsid\{a6b222ab-a5ea-4899-b230-084657eddc7d}[appid]
 Oueries value:
                         HKCR\clsid\{a6b222ab-a5ea-4899-b230-
084657eddc7d}\inprocserver32[threadingmodel]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
 Queries value:
                         HKCU\software\microsoft\internet explorer\zoom[resettextsizeonstartup]
 Queries value:
                         HKCU\software\microsoft\internet explorer\zoom[resettextsizeonzoom]
                         HKCU\software\microsoft\internet explorer\zoom[resetzoomonstartup2]
 Oueries value:
 Queries value:
                         HKCU\software\microsoft\internet explorer\zoom[zoomfactor]
 Queries value:
                         HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
 Oueries value:
 Queries value:
                         HKLM\software\policies\microsoft\internet explorer[smartdithering]
 Queries value:
                         HKCU\software\microsoft\internet explorer[smartdithering]
                         HKCU\software\microsoft\internet explorer[rtfconverterflags]
 Oueries value:
 Queries value:
                         HKLM\software\policies\microsoft\internet explorer\main[usecleartype]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[usecleartype]
                         HKLM\software\policies\microsoft\internet
 Oueries value:
explorer\main[page_transitions]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[page_transitions]
 Oueries value:
                         HKLM\software\policies\microsoft\internet
explorer\main[use_dlgbox_colors]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
 Oueries value:
                         HKLM\software\policies\microsoft\internet explorer\main[anchor
underline]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[anchor underline]
                         HKCU\software\microsoft\internet explorer\main[css_compat]
 Oueries value:
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[expand alt text]
 Queries value:
                         HKLM\software\policies\microsoft\internet explorer\main[display inline
images]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[display inline images]
 Queries value:
                         HKLM\software\policies\microsoft\internet explorer\main[display inline
videos1
                         HKCU\software\microsoft\internet explorer\main[display inline videos]
 Queries value:
 Oueries value:
                         HKLM\software\policies\microsoft\internet
explorer\main[play_background_sounds]
                         HKCU\software\microsoft\internet explorer\main[play_background_sounds]
 Queries value:
                         HKLM\software\policies\microsoft\internet explorer\main[play_animations]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[play_animations]
 Oueries value:
                         HKLM\software\policies\microsoft\internet
 Queries value:
explorer\main[print_background]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[print_background]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[use stylesheets]
 Queries value:
                         HKLM\software\policies\microsoft\internet explorer\main[smoothscroll]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[smoothscroll]
 Queries value:
                         HKLM\software\policies\microsoft\internet explorer\main[xmlhttp]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[xmlhttp]
 Oueries value:
                         HKLM\software\policies\microsoft\internet explorer\main[show image
placeholders]
                         HKCU\software\microsoft\internet explorer\main[show image placeholders]
 Oueries value:
                         HKLM\software\policies\microsoft\internet explorer\main[disable script
 Queries value:
debugger]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[disable script debugger]
 Oueries value:
                         HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[move system caret]
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[force offscreen
composition]
                         HKLM\software\policies\microsoft\internet explorer\main[enable
 Oueries value:
autoimageresize]
                         HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
 Oueries value:
 Queries value:
                         HKCU\software\microsoft\internet explorer\main[usethemes]
                         HKCU\software\microsoft\internet explorer\main[usehr]
 Oueries value:
```

 $HKCU\software\microsoft\internet\ explorer\main[q300829]$

Queries value:

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

HKLM\software\policies\microsoft\internet explorer\main[xdomainrequest] Oueries value:

Oueries value: HKCU\software\microsoft\internet explorer\main[xdomainrequest] HKLM\software\microsoft\internet explorer\main[xdomainrequest] Queries value: HKLM\software\policies\microsoft\internet explorer\main[domstorage] Oueries value:

Queries value: HKCU\software\microsoft\internet explorer\main[domstorage] Oueries value: HKLM\software\microsoft\internet explorer\main[domstorage]

HKCU\software\microsoft\internet Oueries value:

explorer\international[default_codepage]

HKCU\software\microsoft\internet explorer\international[autodetect] Oueries value:

Oueries value: HKCU\software\microsoft\internet explorer\international\scripts[default_iefontsizeprivate]

Oueries value: HKCU\software\microsoft\internet explorer\settings[anchor color] Oueries value: HKCU\software\microsoft\internet explorer\settings[anchor color visited]

Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color hover] Queries value: HKCU\software\microsoft\internet explorer\settings[always use my colors] Oueries value: HKCU\software\microsoft\internet explorer\settings[always use my font

size]

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

face1

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

hyperlinks]

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

color]

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

programmatic cut_copy_paste]

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

HKCU\software\microsoft\internet Oueries value:

explorer\international\scripts\3[iefontsize]

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

Oueries value: HKCU\software\microsoft\internet

explorer\international\scripts\3[iefixedfontname]

HKCU\software\microsoft\internet explorer\international[acceptlanguage] Oueries value: HKCR\interface\{48a98a1f-5cdd-47ee-9286-db04a3eb7ce1}\proxystubclsid32[] Oueries value:

HKLM\software\microsoft\internet explorer\version vector[vml] Queries value: HKLM\software\microsoft\internet explorer\version vector[ie] Queries value:

Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[iexplore.exe]

Oueries value: HKCU\software\microsoft\internet explorer\browseremulation[allsitescompatibilitymode] HKCU\software\microsoft\internet Oueries value: explorer\browseremulation[intranetcompatibilitymode] Queries value: HKCU\software\microsoft\internet explorer\browseremulation[localmachinecompatibilitymode]

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

settings\5.0\user agent[]

HKLM\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\user agent[]

Queries value:

HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent[compatible]

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

settings\5.0\user agent[compatible] HKCU\software\microsoft\windows\currentversion\internet

Queries value:

settings\5.0\user agent[version] Oueries value: HKLM\software\microsoft\windows\currentversion\internet

settings\5.0\user agent[version]

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

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

settings\5.0\user agent[platform]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\user agent[platform]

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

settings\zones\3[2700]

Queries value:

agent]

HKLM\software\microsoft\windows\currentversion\internet settings\zones\3[2700]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_xssfilter[iexplore.exe] HKCU\software\microsoft\windows\currentversion\internet Oueries value:

settings\zones[securitysafe]

Queries value:

HKCR\clsid\{00020420-0000-0000-c000-Oueries value:

00000000046}\inprocserver32[inprocserver32]

HKCR\clsid\{00020420-0000-0000-c000-00000000046}\inprocserver32[] Queries value:

HKCR\clsid\{00020420-0000-0000-c000-00000000046}[appid] Oueries value:

Oueries value: HKCR\clsid\{00020420-0000-0000-c000-

00000000046}\inprocserver32[threadingmodel]

HKCR\clsid\{9ba05972-f6a8-11cf-a442-Oueries value:

00a0c90a8f39}\inprocserver32[inprocserver32]

 $HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\tinprocserver32[]$ Oueries value:

HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[appid] Oueries value:

Oueries value: HKCR\clsid\{9ba05972-f6a8-11cf-a442-

00a0c90a8f39}\inprocserver32[threadingmodel]

Oueries value: HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\proxystubclsid32[]

Queries value: HKCR\clsid\{00020424-0000-0000-c000-

00000000046}\inprocserver32[inprocserver32]

HKCR\clsid\{00020424-0000-0000-c000-00000000046}\inprocserver32[] Oueries value:

HKCR\clsid\{00020424-0000-0000-c000-00000000046}[appid] Oueries value:

HKCR\clsid\{00020424-0000-0000-c000-Oueries value:

00000000046}\inprocserver32[threadingmodel]

HKCR\interface\{d30c1661-cdaf-11d0-8a3e-00c04fc9e26e}\typelib[] Queries value: Oueries value: $HKCR \setminus \{d30c1661 - cdaf - 11d0 - 8a3e - 00c04fc9e26e\} \setminus \{typelib[version]\}$ HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[] Oueries value: Queries value: HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[]

Queries value: HKLM\software\microsoft\rpc[udtalignmentpolicy]

HKCR\interface\{6d5140c1-7436-11ce-8034-00aa006009fa}\proxystubclsid32[] Oueries value:

Queries value: HKCR\clsid\{b8da6310-e19b-11d0-933c-

00a0c90dcaa9}\inprocserver32[inprocserver32]

HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}\inprocserver32[] Queries value:

Queries value: HKCR\clsid\{b8da6310-e19b-11d0-933c-00a0c90dcaa9}[appid]

Queries value: HKCR\clsid\{b8da6310-e19b-11d0-933c-

00a0c90dcaa9}\inprocserver32[threadingmodel]

Queries value: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]

Queries value: HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[] HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[version] Queries value: Queries value: HKCU\software\microsoft\internet explorer\toolbar[menuuserexpanded]

HKCU\software\microsoft\windows\currentversion\internet

settings[warnonintranet]

Queries value:

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

settings[warnonintranet]

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

settings\zonemap[autodetect]

Queries value: HKCR\interface\{9d973e3b-f610-4f03-83d3-

aed90c3237ac}\synchronousinterface[]

 $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8$ Queries value: c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable]

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

settings\zones\3[1c00]

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

settings\zones\3[1207]

HKCR\clsid\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[appid] Queries value: HKCU\software\microsoft\windows\currentversion\internet Oueries value:

settings[cointernetcombineiuricachesize]

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

settings[cointernetcombineiuricachesize]

Queries value: HKLM\software\microsoft\internet explorer\activex compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[compatibility flags] HKLM\software\microsoft\internet explorer\activex Oueries value: compatibility\{08b0e5c0-4fcb-11cf-aaa5-00401c608501}[miscstatus flags]

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

settings\zones\3[120b]

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

settings\zones\3[1208]

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

settings\zones\3[2201]

Queries value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-

abcdeffedcbb}\inprocserver32[inprocserver32]

HKCR\clsid\{cafeefac-0017-0000-0002-Oueries value:

abcdeffedcbb}\inprocserver32[inprocserver32]

Queries value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002abcdeffedcbb}\inprocserver32[]

HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-Queries value:

abcdeffedcbb}[appid]

HKCR\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}[appid] Queries value: HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-Oueries value:

abcdeffedcbb}\inprocserver32[threadingmodel]

Queries value: HKLM\software\javasoft\java runtime environment\1.7.0_02[eula] Queries value: HKLM\software\javasoft\java plug-in\10.2.0[usejava2iexplorer]

Oueries value:

11cf-aaa5-00401c608501}\iexplore[count]

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

settings\zones\3[1201]

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

options\jvm.dll[checkapphelp]

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

settings\zones\3[2000]

Oueries value: HKCR\htmlfile\shell[1

Oueries value: HKCR\htmlfile\shell\edit\command[]

Oueries value: HKLM\software\microsoft\internet explorer\default html editor[stubs]

Queries value: HKLM\software\microsoft\internet explorer\default html

editor[description]

Queries value: HKLM\software\microsoft\internet explorer\default html

```
editor\shell\edit[friendlyappname]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm[progid]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.htm[application]
   Queries value:
                                             HKCR\.htm[]
   Oueries value:
                                              HKCR\applications\notepad.exe\shell\edit\command[]
                                              HKCU\software\microsoft\internet explorer\main[checkdocumentforprogid]
   Oueries value:
   Oueries value:
                                              HKLM\software\microsoft\internet explorer\main[checkdocumentforprogid]
                                              HKLM\software\microsoft\internet explorer\feed discovery[enabled]
   Oueries value:
                                              HKCU\software\microsoft\ftp[use web based ftp]
   Oueries value:
   Queries value:
                                             HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowclsidprogidmapping]
                                              HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[docobject]
   Oueries value:
                                              HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[browseinplace]
   Oueries value:
   Queries value:
                                              HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[isshortcut]
   Oueries value:
                                              HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000\}[alwaysshowext]
                                              HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[nevershowext]
   Oueries value:
   Queries value:
                                              HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}\inprocserver32[]
   Queries value:
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-
444553540000}\inprocserver32[loadwithoutcom]
                                             HKLM\software\microsoft\windows\currentversion\shell
   Queries value:
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
                                             HKCU\software\microsoft\windows\currentversion\shell
   Queries value:
extensions\blocked[{ff393560-c2a7-11cf-bff4-444553540000}]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
                                             HKLM\software\microsoft\windows\currentversion\shell
   Queries value:
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x4011
                                             HKCU\software\microsoft\windows\currentversion\shell
   Queries value:
extensions\cached[{ff393560-c2a7-11cf-bff4-444553540000} {e022b1e2-a19e-4b43-8160-7bcecacb3d6e}
0x4011
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-
   Queries value:
444553540000}\inprocserver32[inprocserver32]
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-444553540000}[appid]
   Oueries value:
                                             HKCR\clsid\{ff393560-c2a7-11cf-bff4-
   Queries value:
444553540000}\inprocserver32[threadingmodel]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\mshist012016032920160330[cacherepair]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\mshist012016032920160330[cachepath]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\mshist012016032920160330[cacheprefix]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cachelimit]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\mshist012016032920160330[cacheoptions]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsfordisplay]
   Queries value:
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
   Oueries value:
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[callforattributes]
   Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-444, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 1944, 19
08002b30309d}1
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hidefolderverbs]
                                             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
   Oueries value:
                                              HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
   Queries value:
   Oueries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\shell32.dll,-9216]
                                              HKLM\software\microsoft\internet explorer\main[maxrenderline]
   Oueries value:
                                              HKLM\software\policies\microsoft\internet explorer\main[use formsuggest]
   Queries value:
   Oueries value:
                                              HKCU\software\microsoft\internet explorer\main[use formsuggest]
   Queries value:
                                              HKLM\software\microsoft\internet explorer\main[use formsuggest]
                                              \label{lem:hkcu} \mbox{HKCU\software\mbox{$^{08}$b0e5c0-4fcb-$}} \mbox{$^{08}$b0e5c0-4fcb-$} \mbox{$^{08}$b0e5c0
   Oueries value:
11cf-aaa5-00401c608501}\iexplore[type]
                                              HKCU\software\microsoft\internet explorer\caretbrowsing[enableonstartup]
   Oueries value:
   Oueries value:
                                              HKCU\software\microsoft\internet explorer\suggested sites[migrationtime]
   Queries value:
                                             HKLM\software\microsoft\internet explorer\migration[ie installed date]
   Queries value:
                                             HKCU\software\microsoft\internet
explorer\main[ie8runonceperinstallcompleted]
                                              HKCU\software\microsoft\internet explorer\main[ie8runoncecompletiontime]
   Queries value:
                                              HKCU\software\microsoft\internet explorer\main[check_associations]
   Oueries value:
   Oueries value:
                                              HKLM\software\microsoft\internet explorer\main[check_associations]
   Oueries value:
                                              HKCR\http[editflags]
   Queries value:
                                              HKCR\http[url protocol]
   Oueries value:
                                              HKCR\http[webnavigableclsid]
```

Queries value:

HKCR\https[editflags]

```
Oueries value:
                          HKCR\https[url protocol]
 Oueries value:
                          HKCR\ftp[editflags]
 Oueries value:
                          HKCR\ftp[url protocol]
                          HKCR\internetshortcut[editflags]
 Queries value:
 Oueries value:
                          HKCR\internetshortcut\defaulticon[]
 Queries value:
                          HKCR\.htm[content type]
 Oueries value:
                          HKCR\http\shell\open\command[]
                          HKCR\http\shell\open\ddeexec[]
 Oueries value:
 Oueries value:
                          HKCR\http\shell\open\ddeexec[noactivatehandler]
                          HKCR\http\shell\open\ddeexec\application[]
 Oueries value:
                          HKCR\http\shell\open\ddeexec\topic[]
 Oueries value:
 Queries value:
                          HKCR\https\shell\open\command[]
 Oueries value:
                          HKCR\https\shell\open\ddeexec[]
                          HKCR\https\shell\open\ddeexec[noactivatehandler]
 Oueries value:
 Queries value:
                          HKCR\https\shell\open\ddeexec\application[]
 Oueries value:
                          HKCR\https\shell\open\ddeexec\topic[]
                          HKCR\ftp\shell\open\command[]
 Queries value:
 Queries value:
                          HKCR\ftp\shell\open\ddeexec[]
 Oueries value:
                          HKCR\ftp\shell\open\ddeexec\ifexec[]
 Oueries value:
                          HKCR\ftp\shell\open\ddeexec[noactivatehandler]
 Queries value:
                          HKCR\ftp\shell\open\ddeexec\application[]
 Queries value:
                          HKCR\ftp\shell\open\ddeexec\topic[]
 Queries value:
                          HKCR\htmlfile\shell\open[]
 Queries value:
                          HKCR\htmlfile\shell\open[muiverb]
 Queries value:
                          HKCR\htmlfile\shell\open\command[]
 Oueries value:
                          HKCR\htmlfile\shell\open\ddeexec[]
 Queries value:
                          HKCR\htmlfile\shell\open\ddeexec[noactivatehandler]
 Queries value:
                          HKCR\htmlfile\shell\open\ddeexec\application[]
                          HKCR\htmlfile\shell\open\ddeexec\topic[]
 Oueries value:
 Queries value:
                          HKCR\mhtmlfile\shell[]
 Queries value:
                          HKCR\htmlfile\shell\opennew[]
                          HKCR\htmlfile\shell\opennew[muiverb]
 Queries value:
                          HKCR\htmlfile\shell\opennew\command[]
 Queries value:
 Queries value:
                          HKCR\htmlfile\shell\opennew\ddeexec[]
                          HKCR\htmlfile\shell\opennew\ddeexec\ifexec[]
 Oueries value:
                          HKCR\htmlfile\shell\opennew\ddeexec[noactivatehandler]
 Queries value:
                          HKCR\htmlfile\shell\opennew\ddeexec\application[]
 Oueries value:
 Oueries value:
                          HKCR\htmlfile\shell\opennew\ddeexec\topic[]
 Queries value:
                          HKCR\.mht[]
                          HKCR\.mht[content type]
 Queries value:
 Oueries value:
                          HKCR\.mhtml[]
                          HKCR\.mhtml[content type]
 Queries value:
                          HKCR\mhtmlfile\shell\open[]
 Oueries value:
                          HKCR\mhtmlfile\shell\open[muiverb]
 Oueries value:
                          HKCR\mhtmlfile\shell\open\command[]
 Oueries value:
                          HKCR\mhtmlfile\shell\open\ddeexec[]
 Queries value:
                          HKCR\mhtmlfile\shell\open\ddeexec\application[]
 Oueries value:
 Queries value:
                          HKCR\mhtmlfile\shell\open\ddeexec\topic[]
 Oueries value:
                          HKCR\mhtmlfile\shell\opennew[]
 Oueries value:
                          HKCR\mhtmlfile\shell\opennew[muiverb]
                          HKCR\mhtmlfile\shell\opennew\command[]
 Oueries value:
                          HKCR\mhtmlfile\shell\opennew\ddeexec[]
 Oueries value:
 Oueries value:
                          HKCR\mhtmlfile\shell\opennew\ddeexec\ifexec[]
                          HKCR\mhtmlfile\shell\opennew\ddeexec[noactivatehandler]
 Queries value:
 Oueries value:
                          HKCR\mhtmlfile\shell\opennew\ddeexec\application[]
 Queries value:
                          HKCR\mhtmlfile\shell\opennew\ddeexec\topic[]
 Oueries value:
                          HKCR\.url[]
                          HKCR\internetshortcut\clsid[]
 Oueries value:
 Queries value:
                          HKCR\internetshortcut\shell\open[clsid]
                          HKCR\internetshortcut\shell\open[legacydisable]
 Queries value:
 Queries value:
                          HKCR\internetshortcut\shell\open\command[]
 Oueries value:
                          HKCR\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837}[]
                          \label{local-bound} HKCR\clsid\{3dc7a020-0acd-11cf-a9bb-00aa004ae837\}[friendlytypename]
 Queries value:
 Queries value:
                          HKCR\applications\iexplore.exe\shell\open\command[]
 Queries value:
                          HKCU\software\microsoft\internet explorer\suggested
sites[objectscreated]
 Queries value:
                          HKCU\software\microsoft\internet explorer\suggested sites[slicepath]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\searchscopes[version]
 Queries value:
                          HKCU\software\microsoft\internet explorer\searchscopes[upgradetime]
 Oueries value:
                          HKLM\software\microsoft\cryptography\defaults\provider types\type
001[name]
                          HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
 Oueries value:
cryptographic provider[type]
 Queries value:
                          HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
 Oueries value:
                          HKLM\software\microsoft\cryptography[machineguid]
 Oueries value:
                          HKCU\software\microsoft\internet explorer\user
preferences[2d53cffc5c1a3dd2e97b7979ac2a92bd59bc839e81]
 Queries value:
                          HKCU\software\microsoft\internet explorer\user
preferences[88d7d0879dab32e14de5b3a805a34f98aff34f5977]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\shell
```

```
folders[local appdata]
                                              HKLM\software\javasoft\java runtime environment\1.7[javahome]
   Oueries value:
   Oueries value:
                                              HKLM\system\wpa\mediacenter[installed]
                                              HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus compatibility 32 [java]
   Queries value:
                                              HKLM\software\microsoft\windows nt\currentversion\ime
   Oueries value:
compatibility[java]
   Queries value:
                                              HKLM\software\microsoft\windows
nt\currentversion\windows[gdiprocesshandlequota]
   Oueries value:
                                              HKCU\software\microsoft\internet
explorer\tabbedbrowsing[quicktabslastused]
                                              HKLM\hardware\devicemap\video[maxobjectnumber]
   Oueries value:
   Queries value:
                                              HKLM\hardware\devicemap\video[\device\video0]
   Oueries value:
                                              HKLM\hardware\devicemap\video[\device\video1]
                                              HKLM\hardware\devicemap\video[\device\video2]
   Oueries value:
   Queries value:
                                              HKLM\software\microsoft\direct3d[geometrydriver]
   Queries value:
                                              HKLM\software\microsoft\direct3d[loaddebugruntime]
                                              HKLM\software\microsoft\direct3d[forcedriverflagsoff]
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-
9b1f4867732a}\0000[installeddisplaydrivers]
                                              HKLM\system\currentcontrolset\control\watchdog\display[earecovery]
   Queries value:
   Queries value:
                                              HKLM\system\currentcontrolset\control\watchdog\display[fullrecovery]
   Queries value:
                                              HKLM\software\microsoft\direct3d\drivers[softwareonly]
   Oueries value:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[java.exe]
                                             HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[*]
   Queries value:
                                              HKLM\software\javasoft\java update\policy[promptautoupdatecheck]
   Queries value:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[java.exe]
                                              HKCU\control panel\desktop[fontsmoothingorientation]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg 2]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\thememanager[themeactive]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\thememanager[dllname]
   Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\thememanager[sizename]
                                              HKCU\software\microsoft\windows\currentversion\thememanager[colorname]
   Queries value:
   Sets/Creates value:
                                              HKCU\software\microsoft\internet explorer\recovery\active[{3af75143-
f55e-11e5-ae32-08002719344d}1
                                              Sets/Creates value:
c9633f71be64\\ \label{language} c9633f71be64\\ \label{language} \label{language} c9633f71be64\\ \label{language} \label{languagee} \label{languagee} \label{lang
   Sets/Creates value:
                                              \label{localization} \begin{tabular}{ll} HKCU software \classes \clsid \cafeefac-0017-0000-0002-abcdeffedcba \clsid \cafeefac-0017-0000-0002-abcdeffedcba \clsid \cafeefac-0017-0000-0002-abcdeffedcba \clid{ll} \clid
                                              HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
   Sets/Creates value:
abcdeffedcba}\inprocserver32[]
   Sets/Creates value:
                                              HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcba}\inprocserver32[threadingmodel]
                                              HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbb}[]
   Sets/Creates value:
   Sets/Creates value:
                                              HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
abcdeffedcbb}\inprocserver32[]
                                              HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
  Sets/Creates value:
abcdeffedcbb}\inprocserver32[threadingmodel]
                                              HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-abcdeffedcbc}[]
   Sets/Creates value:
                                              HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
   Sets/Creates value:
abcdeffedcbc}\inprocserver32[]
                                              HKCU\software\classes\clsid\{cafeefac-0017-0000-0002-
   Sets/Creates value:
abcdeffedcbc}\inprocserver32[threadingmodel1
   Sets/Creates value:
                                              HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-abcdeffedcba}[]
                                              HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-
   Sets/Creates value:
abcdeffedcba}\inprocserver32[1
   Sets/Creates value:
                                              HKCU\software\classes\clsid\{cafeefac-0017-0000-ffff-
abcdeffedcba}\inprocserver32[threadingmodel]
   Sets/Creates value:
                                              HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-00805f499d93}[]
   Sets/Creates value:
                                              HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-
00805f499d93}\inprocserver32[]
   Sets/Creates value:
                                              HKCU\software\classes\clsid\{8ad9c840-044e-11d1-b3e9-
00805f499d93}\inprocserver32[threadingmodel]
                                              HKCU\software\classes\javaplugin.1020\clsid[]
   Sets/Creates value:
   Sets/Creates value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cachepath]
  Sets/Creates value:
                                              \label{lem:hkcu} \verb+KCU\+software\+microsoft\+windows\+currentversion\+internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cacheprefix]
   Sets/Creates value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cachelimit]
  Sets/Creates value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012016032920160330[cacheoptions]
  Sets/Creates 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\mshist012016032920160330[cacherepair]
   Value changes:
                                              HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:
                                              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Value changes:
                                              HKCU\software\microsoft\windows\currentversion\explorer\shell
```

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

folders[cookies]
 Value changes:
folders[history]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[desktop]

Value changes: HKCU\software\microsoft\internet explorer\main[compatibilityflags] Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[favorites]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]

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

settings\zones[securitysafe]

Value changes:

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

806d6172696f}[baseclass]

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\explorer\shell

folders[local appdata]

HKCU\software\microsoft\internet explorer\main\windowssearch[version] Value changes: Value changes: HKCR\typelib\{1ea4dbf0-3c3b-11cf-810c-00aa00389b71}\1.1\0\win32[] Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{e2e2dd38-d088-

4134-82b7-f2ba38496583}\iexplore[type]

Value changes:

4134-82b7-f2ba38496583}\iexplore[count]

Value changes:

4134-82b7-f2ba38496583}\iexplore[time]

HKCU\software\microsoft\windows\currentversion\ext\stats\{fb5f1910-f110-Value changes:

11d2-bb9e-00c04f795683}\iexplore[type]

Value changes:

11d2-bb9e-00c04f795683}\iexplore[count]

Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{fb5f1910-f110-

11d2-bb9e-00c04f795683}\iexplore[time]

HKCU\software\microsoft\internet explorer\main[fullscreen] Value changes: Value changes: HKCU\software\microsoft\internet explorer\main[window_placement]

HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-Value changes:

4283-a596-fa578c2ebdc3}\iexplore[type]

Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-

4283-a596-fa578c2ebdc3}\iexplore[count] HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-Value changes:

4283-a596-fa578c2ebdc3}\iexplore[time]

Value changes:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \ext \stats \colored \colored$ 4283-a596-fa578c2ebdc3}\iexplore[loadtime]

Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{18df081c-e8ad-

4283-a596-fa578c2ebdc3}\iexplore[loadtimecount] HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-

Value changes:

435b-bc74-9c25c1c588a9}\iexplore[type]

Value changes:

435b-bc74-9c25c1c588a9}\iexplore[count1

Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{dbc80044-a445-

435b-bc74-9c25c1c588a9}\iexplore[time] Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-

11cf-aaa5-00401c608501}\iexplore[type]

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \ext\stats \end{tabular} \label{lem:hkcu} \end{tabular} Abbout \subseteq \current \$ Value changes:

11cf-aaa5-00401c608501}\iexplore[count]

Value changes: HKCU\software\microsoft\windows\currentversion\ext\stats\{08b0e5c0-4fcb-

11cf-aaa5-00401c608501}\iexplore[time]

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

settings\5.0\cache\extensible cache\mshist012016032920160330[cachepath]

Value changes: HKCU\software\microsoft\direct3d\mostrecentapplication[name]