## Malware Analysis Appliance by Blue Coat Systems, Inc. Task Details Host: mag2, Sample ID: 470, Task ID: 479 Task ID: 479 Risk Level: 10 Date Processed: 2016-03-24 14:07:57 (UTC) Processing Time: 61.63 seconds Virtual Environment: IntelliVM **Execution Arguments:** "c:\windows\temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe" Sample ID: 470 basic Type: Owner: admin Label: 755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63 Date Added: 2016-03-24 14:07:57 (UTC) File Type: PE32:win32:gui 1580101 bytes File Size: cba74e507e9741740d251b1fb34a1874 MD5: SHA256: 755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63 Description: Pattern Matching Results 3 Writes to a log file [Info] 10 Creates malicious events: Bookworm [Worm] 5 Creates process in suspicious location Attempts to connect to dynamic DNS 6 Creates executable in application data folder 6 Modifies registry autorun entries Starts sychost.exe Connects to local host 5 Possible process injection 5 Installs service Opens Copy Hook Handlers key 3 Long sleep detected 1 YARA score 1 Terminates third-party processes 6 Starts process from Application Data folder Static Events YARA rule hit: Nonexecutable Anomaly: PE: Contains a virtual section Process/Thread Events Creates process: $\hbox{C:$\WINDOWS\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe} \\$ $["c:\windows\temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe"]$ C:\Program Files\flashplayer18\_a\_install.exe ["C:\Program Files\flashplayer18\_a\_install.exe" ] Creates process: C:\Program Files\install.exe ["C:\Program Files\install.exe" ] Creates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\MsMpEng.exe ["C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\MsMpEng.exe" "C:\Program Files\install.exe" ] C:\Documents and Settings\All Users\Application Creates process: Data\Microsoft\DeviceSync\MsMpEng.exe ["C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MsMpEng.exe"] C:\WINDOWS\system32\svchost.exe [ -main] Creates process: C:\WINDOWS\system32\svchost.exe [ -protect] C:\WINDOWS\system32\dllhost.exe [C:\WINDOWS\System32\dllhost.exe -user] Creates process: Creates process: PID:1656 C:\WINDOWS\system32\svchost.exe Writes to process: PID:832 C:\WINDOWS\system32\svchost.exe Writes to process: PID:1096 C:\WINDOWS\system32\dllhost.exe Writes to process: Terminates process: C:\WINDOWS\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe C:\Documents and Settings\All Users\Application Terminates process: Data\Microsoft\DeviceSync\MsMpEng.exe C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\MsMpEng.exe Terminates process: Terminates process: C:\Program Files\install.exe Named Object Events

,
\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-
\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-
\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-
\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-
488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
\BaseNamedObjects\ZonesCounterMutex
\BaseNamedObjects\ZoneAttributeCacheCounterMutex
\BaseNamedObjects\ZonesCacheCounterMutex
\BaseNamedObjects\ZonesLockedCacheCounterMutex
\BaseNamedObjects\oleacc-msaa-loaded
\BaseNamedObjects\Adobe_ADM.log
\BaseNamedObjects\c:!documents and settings!admin!local
/ 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\!PrivacIE!SharedMemorv!Mutex \BaseNamedObjects\ SHuassist.mtx Creates mutex: Creates mutex: \BaseNamedObjects\BB6cmqyHzy8kkcJ \BaseNamedObjects\SHIMLIB\_LOG\_MUTEX Creates mutex: \BaseNamedObjects\DDrawWindowListMutex Creates mutex: \BaseNamedObjects\DDrawDriverObjectListMutex Creates mutex: Creates mutex: \BaseNamedObjects\\_\_DDrawExclMode Creates mutex: \BaseNamedObjects\\_\_DDrawCheckExclMode\_\_ \BaseNamedObjects\Adobe\_GDE.log Creates mutex: Creates event: \BaseNamedObjects\DINPUTWINMM \BaseNamedObjects\userenv: User Profile setup event Creates event: Creates event: \BaseNamedObjects\ShellCopyEngineRunning Creates event: \BaseNamedObjects\ShellCopyEngineFinished \BaseNamedObjects\CancelPort{1A294DC5-2893-48DA-8D21-A405C1A6E549} Creates event: Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57} Creates semaphore: \BaseNamedObjects\{61410B1E-728E-4E96-96DD-9BE271228D74} Creates semaphore: \BaseNamedObjects\{A925355A-7A05-4070-B3BC-3D323F229F91}} File System Events Creates: C:\Documents and Settings\Admin\Local Settings\Temp\\$inst Creates: C:\Documents and Settings\Admin\Local Settings\Temp\\$inst\2.tmp Creates: C:\Documents and Settings\Admin\Local Settings\Temp\\$inst\temp\_0.tmp C:\Program Files\install.exe Creates: Creates: C:\Program Files\flashplayer18\_a\_install.exe C:\Program Files\Adobe\NewProduct Creates: C:\Program Files\Adobe\NewProduct\Uninstall.exe Creates: C:\Program Files\Adobe\NewProduct\Uninstall.ini Creates: Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\E8127C44-F7F4-4DCB-8787-6503FDE881E8 Creates: C:\Program Files Creates: C:\DOCUME~1 Creates: C:\DOCUME~1\Admin Creates: C:\DOCUME~1\Admin\LOCALS~1 C:\DOCUME~1\Admin\LOCALS~1\Temp Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0 Creates: C:\Documents and Settings\Admin\Local Settings\Temp\Adobe\_ADMLogs Creates: C:\Documents and Settings\Admin\Local Creates:  $Settings \verb|\Temp\RarSFX0\_\_tmp\_rar\_sfx\_access\_check\_78092$ C:\Documents and Settings\Admin\Local Creates: Settings\Temp\Adobe\_ADMLogs\Adobe\_ADM.log C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFXO\MpSvc.dll Creates: Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFXO\readme.txt C:\Documents and Settings\Admin\Local Settings\Temporary Internet Creates: Files\Content.IE5\QXMNQBKF\160[1] C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0 C:\Documents and Settings Creates: C:\Documents and Settings\All Users Creates: Creates: C:\Documents and Settings\All Users\Application Data C:\Documents and Settings\All Users\Application Data\Microsoft Creates: Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync Creates: C:\Documents and Settings\All Users\Application Data\Mozilla C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto Creates: Creates:  $\label{lem:c:Documents} C:\Documents\ and\ Settings\All\ Users\Application\ Data\Mozilla\Crypto\RSA$ Creates: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA\MachineKeys Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MsMpEng.exe C:\Documents and Settings\All Users\Application Creates: Data\Microsoft\DeviceSync\MpSvc.dll C:\Documents and Settings\All Users\Application Creates: Data\Microsoft\DeviceSync\delete.txt C:\Documents and Settings\All Users\Application Creates: Data\Mozilla\Crypto\RSA\MachineKeys\sgkey.data Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MpSvc C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4 C:\Documents and Settings\All Users\Application Creates: Data\Mozilla\Crypto\RSA\MachineKeys\889EC630 C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\warning\_icon\_200.png C:\Documents and Settings\Admin\Local Settings\Application Creates: Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status\_icon\_caution\_200.png Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status\_icon\_caution\_100.png Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status\_icon\_caution\_125.png Creates:  ${\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}$ Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status\_icon\_caution\_150.png

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

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

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

Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status\_icon\_x\_200.png

Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status\_icon\_x\_100.png

Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status\_icon\_x\_125.png

Creates:

Creates:

Creates:

```
Creates:
                          C:\Documents and Settings\Admin\Local Settings\Application
\label{lem:decomposition} Data \land Adobe \land F9B18643-0BCF-418A-9448-0879E97604E4 \land status\_icon\_x\_150.png
 Creates:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_check_200.png
 Creates:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_check_100.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_check_125.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status icon check 150.png
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_darkgray_base_200.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_darkgray_base_100.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_blue_active_200.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_blue_active_100.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_blue_active_125.png
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_blue_active_150.png
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Application
\label{lem:decomposition} Data \land Adobe \land F9B18643-0BCF-418A-9448-0879E97604E4 \land transparent.gif
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data \land Adobe \land F9B18643 - 0BCF - 418A - 9448 - 0879E97604E4 \land gray\_button\_200.png
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\close_200.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_pole_null_200.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_pole_null_100.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_pole_null_125.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_pole_null_150.png
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_200.png
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_100.png
                          C:\Documents and Settings\All Users\Application
Data\Microsoft\Crypto\RSA\MachineKeys\5227f4c3bk
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_125.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_150.png
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_mini_200.png
 Creates
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
\label{low_button_mini_100.png} Data \land Adobe \land F9B18643-0BCF-418A-9448-0879E97604E4 \land yellow\_button\_mini\_100.png
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_mini_125.png
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_mini_150.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_short_200.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_short_100.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Creates:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_short_125.png
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_short_150.png
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\info_icon_100.png
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Creates:
Files\Content.IE5\CXCXW1MR\SC[1]
                          C:\DOCUME~1\Admin\LOCALS~1\Temp\Adobe_ADMLogs
 Creates:
 Creates
                          C:\Documents and Settings\Admin\Local
{\tt Settings\Temp\Adobe\_ADMLogs\Adobe\_GDE.log}
                          C:\WINDOWS\Prefetch\755A4B2EC15DA6BB01248B2DFBAD2-0DD218E0.pf
 Opens:
 Opens:
                          C:\Documents and Settings\Admin
                          C:\WINDOWS\svstem32\winmm.dll
 Opens:
                          C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls 6595b64144ccf1df 6.0.2600.5512 x-ww 35d4ce83
                          C:\WINDOWS\WinSxS\x86 Microsoft.Windows.Common-
 Opens:
Controls 6595b64144ccf1df 6.0.2600.5512 x-ww 35d4ce83\comct132.dll
                          C:\WINDOWS\system32\cabinet.dll
 Opens:
 Opens:
C:\WINDOWS\system32\imm32.dll
 Opens:
 Opens:
                          C:\WINDOWS\WindowsShell.Manifest
 Opens:
                          C:\WINDOWS\WindowsShell.Config
                          C:\WINDOWS\system32\shell32.dll
 Opens:
                          C:\WINDOWS\system32\shell32.dll.124.Manifest
 Opens:
                          C:\WINDOWS\system32\shell32.dll.124.Config
 Opens:
 Opens:
                          C:\WINDOWS\system32\MSCTF.dll
 Opens:
                          C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temp\$inst
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
 Opens:
                          C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\7.tmp
 Opens:
                          C: \DOCUME~1\Admin\LOCALS~1\Temp\sinst\9.tmp
 Opens:
                          C:\WINDOWS\system32\uxtheme.dll
 Opens:
                          C:\WINDOWS\system32\rpcss.dll
                          C:\WINDOWS\system32\msftedit.dll
 Opens:
```

```
Opens:
                                     C:\WINDOWS\system32\MSIMTF.dll
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
  Opens:
                                     C:\Program Files\install.exe
                                     C:\Program Files\flashplayer18_a_install.exe
  Opens:
                                     C:\Program Files\Adobe\NewProduct\Uninstall.exe
  Opens:
  Opens:
                                     C:\WINDOWS\Temp\4b9b0e12-3c06-4701-a107-684f03fb3d30
                                     C:\Program Files\Adobe\NewProduct
  Opens
  Opens:
                                     C:\WINDOWS\system32\netapi32.dll
  Opens:
                                     C:\Documents and Settings
  Opens:
                                     C:\Documents and Settings\Admin\My Documents\desktop.ini
  Opens:
                                     C:\Documents and Settings\All Users
                                     C:\Documents and Settings\All Users\Documents\desktop.ini
  Opens:
  Opens:
                                     C:\WINDOWS\system32\clbcatq.dll
  Opens:
                                     C:\WINDOWS\system32\comres.dll
                                     C:\WINDOWS\Registration\R00000000007.clb
  Opens:
                                     C:\WINDOWS\system32\urlmon.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\urlmon.dll.123.Manifest
  Opens:
                                     C:\WINDOWS\system32\urlmon.dll.123.Config
  Opens:
                                     C:\WINDOWS\system32\apphelp.dll
  Opens:
                                     C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:
                                     C:\WINDOWS\AppPatch\systest.sdb
  Opens:
                                     C:\Program Files
                                     C:\Program Files\flashplayer18_a_install.exe.Manifest
  Opens:
                                     C:\Program Files\flashplayer18_a_install.exe.Config
  Opens:
                                     C:\WINDOWS\Prefetch\FLASHPLAYER18_A_INSTALL.EXE-0B6F0919.pf
  Opens:
                                     C:\WINDOWS\system32\winhttp.dll
  Opens:
                                     C:\WINDOWS\system32\msi.dll
  Opens:
                                     C:\WINDOWS\system32\psapi.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\msimg32.dll
                                     C:\WINDOWS\system32\winspool.drv
  Opens:
  Opens:
                                     C:\WINDOWS\system32\oledlg.dll
  Opens:
C: \verb|WINDOWS| \verb|WinSxS| x86_Microsoft. | \verb|Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-ww_dfb54e0cf1df_1.0.2600.5512_x-
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-
ww_dfb54e0c\GdiPlus.dll
                                     C:\WINDOWS\system32\crypt32.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\msasn1.dll
                                     C:\WINDOWS\system32\wintrust.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\oleacc.dll
  Opens:
                                     C:\WINDOWS\system32\msvcp60.dll
  Opens:
                                     C:\Program Files\install.exe.Manifest
  Opens:
                                     C:\Program Files\install.exe.Config
                                     C: \DOCUME \sim 1 \land Admin \land LOCALS \sim 1 \land Temp \land sinst \land 0.tmp
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\1.tmp
  Opens:
  Opens:
                                     C:\WINDOWS\Prefetch\INSTALL.EXE-199863BB.pf
                                     C:\WINDOWS\system32\SHELL32.dll.124.Manifest
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\3.tmp
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\4.tmp
  Opens:
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\5.tmp
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\6.tmp
  Opens:
  Opens:
                                     C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\8.tmp
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\10.tmp
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\11.tmp
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\12.tmp
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\13.tmp
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\14.tmp
  Opens:
  Opens:
                                     C: \DOCUME \sim 1 \land Admin \land LOCALS \sim 1 \land Temp \land \$inst \land 15.tmp
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\16.tmp
  Opens:
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\17.tmp
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\20.tmp
  Opens:
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\50.tmp
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\21.tmp
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\51.tmp
  Opens:
                                     C:\WINDOWS\system32\oleaccrc.dll
  Opens:
                                     C:\WINDOWS\system32\riched32.dll
                                     C:\WINDOWS\system32\riched20.dll
  Opens:
                                     C:\WINDOWS\system32\browseui.dll
  Opens:
                                     C:\WINDOWS\system32\browseui.dll.123.Manifest
  Opens:
                                     C:\WINDOWS\system32\browseui.dll.123.Config
  Opens:
                                     C:\WINDOWS\Fonts\SEGOEUI.TTF
  Opens:
                                     {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
  Opens
Data\Adobe\E8127C44-F7F4-4DCB-8787-6503FDE881E8
                                     C:\WINDOWS\system32\ntmarta.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\samlib.dll
  Opens:
                                     C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\Adobe_ADMLogs\Adobe_ADM.log
  Opens:
  Opens:
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\RarSFX0\__tmp_rar_sfx_access_check_78092
                                     C:\Documents and Settings\Admin\Local
Settings\Temp\Adobe_ADMLogs\Adobe_ADM.log
  Opens:
                                     C:\Program Files\flashplayer18_a_install.exe.3.Manifest
                                     C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe
  Opens:
  Opens:
                                     C:\WINDOWS\system32\ieframe.dll
  Opens:
                                     C:\Program Files\Internet Explorer\iexplore.exe
  Opens:
                                     {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\RarSFX0\MpSvc.dll}
  Opens:
                                     C:\WINDOWS\system32\ieframe.dll.123.Manifest
  Opens:
                                     C:\WINDOWS\system32\ieframe.dll.123.Config
  Opens:
                                     C:\WINDOWS\system32\en-US\ieframe.dll.mui
                                     {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\RarSFX0\readme.txt}
  Opens:
```

Opens:

Opens:

Opens:

C:\WINDOWS\win.ini

C:\

C:\WINDOWS\system32\setupapi.dll

```
Opens:
                         C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
                          C:\WINDOWS\system32\WININET.dll.123.Config
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IF5
                          C:\Documents and Settings\Admin\Local Settings\History
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5\index.dat
                         C:\Documents and Settings\Admin\Cookies
 Opens:
                         C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings
                         C:\Documents and Settings\Admin\Local Settings\Temp
 Opens:
 Opens:
                          C:\WINDOWS\system32\mshtml.dll
                         C:\WINDOWS\system32\msls31.dll
 Opens:
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFXO\MsMpEng.exe.Manifest
 Opens:
                         \label{locals-1} C: \DOCUME-1\Admin\LOCALS-1\Temp\RarSFX0\MsMpEng.exe. Config
 Opens:
                         C:\WINDOWS\Prefetch\MSMPENG.EXE-13EF2649.pf
 Opens:
                         C:\WINDOWS\system32\shdocvw.dll
 Opens:
                         C:\WINDOWS\system32\cryptui.dll
 Opens:
                         C:\WINDOWS\system32\CRYPTUI.dll.2.Manifest
                         C:\WINDOWS\system32\CRYPTUI.dll.2.Config
 Opens:
                          C:\WINDOWS\system32\SHDOCVW.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\SHDOCVW.dll.123.Config
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
 Opens:
Files\Content.IE5\QXMNQBKF
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
                         C:\Documents and Settings\All Users\Application
 Opens:
Data\Microsoft\DeviceSync
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\MsMpEng.exe
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\MpSvc.dll
                         C:\Documents and Settings\All Users\Application
Data\Mozilla\Crypto\RSA\MachineKeys
                         C:\Documents and Settings\All Users\Application
Data\Mozilla\Crypto\RSA\MachineKeys\sgkey.data
                         C:\WINDOWS\Prefetch\MSMPENG.EXE-1806D63D.pf
 Opens:
 Opens:
                         C:\WINDOWS\system32
 Opens:
                         C:\WINDOWS\system32\mlang.dll
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Manifest
                         C:\WINDOWS\system32\MLANG.dll.123.Config
 Opens:
                         C:\Documents and Settings\All Users\Application
 Opens:
{\tt Data\Microsoft\DeviceSync\readme.txt}
                         C:\Documents and Settings\All Users\Application
 Opens:
Data\Microsoft\DeviceSync\MpSvc
                         C:\WINDOWS\system32\msxml3.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\svchost.exe
 Opens:
                         C:\WINDOWS
 Opens:
                         C:\WINDOWS\System32\svchost.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf
 Opens:
                         C:\WINDOWS\system32\shimeng.dll
 Opens:
                          C:\WINDOWS\AppPatch\AcGenral.dll
                         C:\WINDOWS\system32\msacm32.dll
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\delete.txt
                         C:\WINDOWS\system32\mydocs.dll
 Opens:
                         C:\WINDOWS\system32\msxml3r.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\mydocs.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\mydocs.dll.123.Config
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\ntshrui.dll
 Opens:
                         C:\WINDOWS\system32\ntshrui.dll
 Opens:
                         {\tt C:\WINDOWS\system32\atl.dll}
                         C:\WINDOWS\system32\ntshrui.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ntshrui.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\jscript.dll
 Opens:
                         C:\WINDOWS\system32\winlogon.exe
 Opens:
                          C:\WINDOWS\system32\xpsp2res.dll
 Opens:
                         C:\WINDOWS\system32\dxtrans.dll
 Opens:
                         C:\WINDOWS\system32\ddrawex.dll
 Opens:
                         C:\WINDOWS\system32\ddraw.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\dciman32.dll
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Mozilla\Crypto\RSA\MachineKeys\889EC630
                         C:\Documents and Settings\All Users\Application
 Opens:
Data\Microsoft\DeviceSync\F45C8A7E
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\s5227f4c3
 Opens:
                         C:\WINDOWS\system32\wtsapi32.dll
 Opens:
                         C:\WINDOWS\system32\winsta.dll
 Opens:
                         C:\WINDOWS\system32\dxtmsft.dll
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
                          C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                          C:\WINDOWS\system32\msv1_0.dll
 Opens:
                          C:\AUTOEXEC.BAT
                         C:\WINDOWS\system32\dllhost.exe
 Opens:
```

```
Opens:
                          C:\Documents and Settings\All Users\Application
Data\Microsoft\Crypto\RSA\MachineKeys\u5227f4c3
                          C:\WINDOWS\System32\dllhost.exe.Manifest
 Opens:
 Opens:
                          C:\WINDOWS\Prefetch\DLLHOST.EXE-45A368CC.pf
 Opens:
                          C:\WINDOWS\system32\sxs.dll
                          C:\WINDOWS\system32\stdole2.tlb
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4
                          C:\WINDOWS\system32\rasapi32.dll
 Opens:
                          C:\WINDOWS\system32\rasman.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\tapi32.dll
 Opens:
                          C:\WINDOWS\system32\rtutils.dll
                          C:\WINDOWS\System32\TAPI32.dll.124.Manifest
 Opens:
                          C:\WINDOWS\System32\TAPI32.dll.124.Config
 Opens:
 Opens:
                          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\sensapi.dll
 Opens:
                          C:\WINDOWS\system32\rasadhlp.dll
 Opens:
                          C:\WINDOWS\system32\dnsapi.dll
 Opens:
                          C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
                          C:\WINDOWS\system32\rsaenh.dll
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR
 Opens:
                          C:\Documents and Settings\Admin\Application
Data\Mozilla\Firefox\profiles.ini
                          C:\Documents and Settings\Admin\Application
 Opens:
Data\Mozilla\Firefox\prefs.js
                          C:\WINDOWS\Fonts\arialbd.ttf
 Opens:
                          C:\DOCUME~1\Admin\LOCALS~1\Temp\Adobe_ADMLogs\Adobe_GDE.log
 Opens:
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\Adobe_ADMLogs\Adobe_GDE.log
                          C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
 Opens:
                          C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                          C:\WINDOWS\system32\schannel.dll
 Opens:
                          C:\WINDOWS\system32\imgutil.dll
                          C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_100.png
                          C:\WINDOWS\system32\pngfilt.dll
                          C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
 Writes to:
                          C:\Program Files\install.exe
 Writes to:
                          C:\Program Files\flashplayer18_a_install.exe
 Writes to:
                          C:\Program Files\Adobe\NewProduct\Uninstall.exe
 Writes to:
                          C:\Program Files\Adobe\NewProduct\Uninstall.ini
 Writes to:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\Adobe_ADMLogs\Adobe_ADM.log
 Writes to:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\RarSFX0\MsMpEng.exe}
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\RarSFX0\MpSvc.dll}
 Writes to:
                          \label{local} \hbox{C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\readme.txt}
 Writes to:
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF\160[1]
                          C:\Documents and Settings\All Users\Application
 Writes to:
Data\Microsoft\DeviceSync\MsMpEng.exe
 Writes to:
                          C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\MpSvc.dll
                          C:\Documents and Settings\All Users\Application
 Writes to:
Data\Microsoft\DeviceSync\delete.txt
 Writes to:
                          C:\Documents and Settings\All Users\Application
Data\Mozilla\Crypto\RSA\MachineKeys\sgkey.data
                          C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\MpSvc
                          C:\Documents and Settings\All Users\Application
 Writes to:
Data\Mozilla\Crypto\RSA\MachineKeys\889EC630
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\warning_icon_200.png
 Writes to:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_caution_200.png
 Writes to
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adohe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_caution_100.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_caution_125.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status icon caution 150.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_x_200.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_x_100.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_x_125.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_x_150.png
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_check_200.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_check_100.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_check_125.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\status_icon_check_150.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
{\tt Data \ Adobe \ F9B18643-0BCF-418A-9448-0879E97604E4 \ progress bar\_darkgray\_base\_200.png}
```

```
Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_darkgray_base_100.png
 Writes to:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
\label{lem:decomposition} Data \land Adobe \land F9B18643-0BCF-418A-9448-0879E97604E4 \land progress bar\_blue\_active\_200.png
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_blue_active_100.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_blue_active_125.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_blue_active_150.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\transparent.gif
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\gray_button_200.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\close_200.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_pole_null_200.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_pole_null_100.png
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\progressbar_pole_null_125.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
\label{lem:decomposition} Data \land Adobe \land F9B18643-0BCF-418A-9448-0879E97604E4 \land progress bar\_pole\_null\_150.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_200.png
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_100.png
                          \hbox{\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}}
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_125.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_150.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_mini_200.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_mini_100.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_mini_125.png
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_mini_150.png
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-OBCF-418A-9448-0879E97604E4\yellow_button_short_200.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_short_100.png
                          C:\Documents and Settings\Admin\Local Settings\Application
 Writes to:
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_short_125.png
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_short_150.png
 Writes to:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\F9B18643-OBCF-418A-9448-0879E97604E4\info_icon_100.png
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
Files\Content.IE5\CXCXW1MR\SC[1]
 Writes to:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\Adobe_ADMLogs\Adobe_GDE.log
 Reads from:
C:\WINDOWS\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
                          C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
 Reads from:
 Reads from:
                          C:\WINDOWS\win.ini
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
                          C:\Documents and Settings\Admin\My Documents\desktop.ini
  Reads from:
                          C:\Documents and Settings\All Users\Documents\desktop.ini
 Reads from
 Reads from:
                          C:\WINDOWS\Registration\R00000000007.clb
                          C:\Program Files\flashplayer18_a_install.exe
 Reads from:
                          C:\Program Files\install.exe
 Reads from:
                          C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\Adobe_ADMLogs\Adobe_ADM.log
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe
 Reads from:
                          C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\readme.txt
 Reads from:
                          C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\MpSvc
 Reads from:
                          C:\Documents and Settings\All Users\Application
Data\Mozilla\Crypto\RSA\MachineKeys\sgkey.data
 Reads from:
                          C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\delete.txt
                          C:\AUTOEXEC.BAT
 Reads from:
                          C:\WINDOWS\system32\dxtmsft.dll
 Reads from:
 Reads from:
                          C:\WINDOWS\system32\stdole2.tlb
 Reads from:
                          C:\WINDOWS\system32\dxtrans.dll
                          C:\WINDOWS\system32\drivers\etc\hosts
 Reads from:
 Reads from
                          C:\WINDOWS\system32\rsaenh.dll
 Reads from:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\Adobe_ADMLogs\Adobe_GDE.log
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\F9B18643-0BCF-418A-9448-0879E97604E4\yellow_button_100.png
                          C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
 Deletes:
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\$inst
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\E8127C44-F7F4-4DCB-8787-6503FDE881E8
 Deletes:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\RarSFX0\__tmp_rar_sfx_access_check_78092
 Deletes:
                          C:\Program Files\install.exe
                          \label{local} \hbox{$C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MpSvc.dll} \\
 Deletes:
                          C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe
```

Deletes:

Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\readme.txt

Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0

Deletes: C:\Documents and Settings\All Users\Application

Data\Microsoft\DeviceSync\delete.txt

## **Network Events**

DNS query: linuxdns.sytes.net DNS query: get.adobe.com DNS query: systeminfothai.gotdns.ch DNS query: sysnc.sytes.net DNS response:  $linuxdns.sytes.net \Rightarrow 0.0.0.0$ DNS response: get.wip4.adobe.com ⇒ 192.150.16.58 DNS response: systeminfothai.gotdns.ch ⇒ 0.0.0.0 DNS response: sysnc.sytes.net  $\Rightarrow$  0.0.0.0 Connects to: 0.0.0.0:80 127.0.0.1:1044 Connects to: Connects to: 0.0.0.0:1433 Connects to: 0.0.0.0:8080 Connects to: 0.0.0.0:53 0.0.0.0:443 Connects to: 192.150.16.58:443 Connects to: Connects to: 0.0.0.0:21 Sends data to: 8.8.8.8:53 Sends data to: 127.0.0.1:1044 Receives data from: linuxdns.sytes.net:0 (0.0.0.0)

## Windows Registry Events

Creates key:

806d6172696f}\

Creates key: HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00

Creates key: folders

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

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

folders

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

Creates kev:

 $HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ user as sist \ \{75048700-ef1f-11d0-9888-1988-1988, 19880, 1988, 1988, 1988, 1988, 1988, 1988, 1988, 1988, 1988, 1988, 1$ 006097deacf9}

Creates key:

 $HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ user as sist \ \{75048700-ef1f-11d0-9888-198860-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19880-19886-19886-19880-19880-$ 006097deacf9}\count

Creates key:

00aa004ae8373

Creates key:

HKCU\software\microsoft\windows\currentversion\explorer\userassist\{5e6ab780-7743-11cf-a12b-

00aa004ae837}\count

Creates key: HKLM\software\classes

HKU\.default\software\microsoft\windows\currentversion\internet\_settings Creates key:

HKU\.default\software\microsoft\multimedia\audio Creates key:

Creates kev: HKU\.default\software\microsoft\multimedia\audio compression manager\

HKU\.default\software\microsoft\multimedia\audio compression Creates kev: manager\msacm

Creates key: HKU\.default\software\microsoft\multimedia\audio compression manager\priority v4.00

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

HKU\s-1-5-21-1757981266-507921405-1957994488-Creates key:

1003\software\microsoft\windows nt\currentversion\winlogon

HKU\s-1-5-21-1757981266-507921405-1957994488-Creates key: 1003\software\microsoft\windows\currentversion\explorer\user shell folders HKU\s-1-5-21-1757981266-507921405-1957994488-Creates key: 1003\software\microsoft\windows\currentversion\explorer\shell folders

Creates key: HKCU\software\microsoft\multimedia\audio Creates key: HKCU\software\microsoft\multimedia\audio compression manager\ Creates key:  $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \mbox{$m$icrosoft \mbox{$m$ultimedia} audio compression manager \mbox{$m$sacm} audio compression manager \$ Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority

v4.00

Deletes value:

Creates key: HKLM\software\microsoft\tracing

Creates key: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\internet settings\connections HKU\s-1-5-21-1757981266-507921405-1957994488-Creates kev: 1003\software\microsoft\windows\currentversion\internet settings HKU\s-1-5-21-1757981266-507921405-1957994488-Creates kev: 1003\software\microsoft\windows nt\currentversion\network\location awareness

HKLM\system\currentcontrolset\services\tcpip\parameters Creates key: HKCU\software\microsoft\windows script\settings Creates key: Deletes value: HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\internet settings[proxyserver]

HKU\s-1-5-21-1757981266-507921405-1957994488-1003\software\microsoft\windows\currentversion\internet settings[proxyoverride]

HKU\s-1-5-21-1757981266-507921405-1957994488-Deletes value: 1003\software\microsoft\windows\currentversion\internet settings[autoconfigurl]

 $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constraint of the$ 

options\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe

```
Opens key:
                                                  HKLM\system\currentcontrolset\control\terminal server
   Opens key:
                                                  HKLM\system\currentcontrolset\control\safeboot\option
   Opens key:
                                                  \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ safer\+ code identifiers
   Opens key:
                                                  HKCU\software\policies\microsoft\windows\safer\codeidentifiers
   Opens key:
HKLM\software\microsoft\windows\currentversion\sidebvside\assemblvstorageroots
   Opens kev:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
Opens key: options\user32.dll
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
                                                  HKLM\system\currentcontrolset\control\session manager
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
   Opens key:
                                                  \label{lem:hklm} \verb+Kklm| software \verb+microsoft| windows nt| current version| image file execution
options\kernel32.dll
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
   Opens key:
                                                  \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
options\msvcrt.dll
Opens key:
options\ole32.dll
                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
   Opens key
                                                  \label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{hicrosoft}\windows nt\currentversion} \mbox{$\mbox{image file execution}$}
options\oleaut32.dll
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.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\cabinet.dll
   Opens key:
                                                  HKLM\system\currentcontrolset\control\error message instrument\
   Opens key:
                                                  HKLM\system\currentcontrolset\control\error message instrument
                                                  \label{lem:hklm} {\tt HKLM \cite{lem:hklm software microsoft windows nt \current version \cite{lem:hklm software lem:hklm lem:hkl
   Opens key:
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\compatibility32
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\ime compatibility
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\windows
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\winlogon
   Opens key:
                                                  HKLM\
   Opens key:
                                                  {\it HKLM} \ {\it Software} \ {\it microsoft} \ {\it windows} \ {\it nt} \ {\it current} \ {\it version} \ {\it ve
   Opens key:
                                                  HKLM\software\microsoft\ole
   Opens key:
                                                  HKCR\interface
                                                  HKCR\interface\{00020400-0000-0000-c000-000000000046}
   Opens key:
   Opens key:
                                                  HKLM\software\microsoft\oleaut
   Opens key:
                                                  HKLM\software\microsoft\oleaut\userera
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32
   Opens kev:
   Opens kev:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
                                                  HKLM\software\microsoft\windows\currentversion\explorer\performance
   Opens key:
                                                  HKCU\
   Opens key:
   Opens key:
                                                  HKCU\software\policies\microsoft\control panel\desktop
   Opens key:
                                                  HKCU\control panel\desktop
                                                  HKCU\software\microsoft\windows\currentversion\explorer\advanced
   Opens key:
   Opens key:
                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ language pack
    Opens key:
                                                  \label{lem:hklm} \mbox{HKLM} \mbox{$\stackrel{\cdot}{\sc hklm}$ irrosoft\windows nt\currentversion\image file execution} \\
   Opens key:
options\msctf.dll
   Opens key:
HKLM \setminus software \\ \setminus compatibility \setminus 755a4b2ec15 \\ da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
   Opens key:
                                                  HKLM\software\microsoft\ctf\systemshared\
   Opens key:
                                                  HKCU\keyboard layout\toggle
   Opens key:
                                                  HKLM\software\microsoft\ctf\
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\imm
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens kev:
options\version.dll
   Opens key:
                                                  HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
   Opens key:
                                                  HKCU\software\microsoft\ctf
                                                  HKLM\software\microsoft\ctf\systemshared
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\uxtheme.dll
   Opens key:
                                                  HKCU\software\microsoft\windows\currentversion\thememanager
   Opens key:
                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msftedit.dll
   Opens kev:
                                                  HKCU\software\microsoft\windows nt\currentversion\windows
                                                  HKLM\software\microsoft\windows
   Opens key:
nt\currentversion\languagepack\surrogatefallback
                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ advanced
   Opens key:
   Opens key:
                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ fontsubstitutes
   Opens key:
                                                  HKLM\software\microsoft\windows\currentversion
   Opens key:
                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ policies\+ explorer
   Opens key
                                                  \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \policies \explorer \end{tabular}
   Opens key:
```

```
a2d8-08002b30309d}
                                     HKCU\software\classes\
  Opens key:
Opens key: HKCl
08002b30309d}\inprocserver32
                                     HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
  Opens kev:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options\setupapi.dll
  Opens key:
                                     HKLM\system\currentcontrolset\control\minint
  Opens kev:
                                     HKLM\svstem\wpa\pnp
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\setup
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\setup\apploglevels
  Opens key:
                                     HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:
                                     HKLM\system\currentcontrolset\services\tcpip\parameters
                                     HKLM\software\policies\microsoft\system\dnsclient
  Opens key:
  Opens key:
                                     HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:
                                     HKLM\software\microsoft\rpc
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key
options\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe\rpcthreadpoolthrottle
  Opens key:
                                     HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
                                     HKLM\system\currentcontrolset\control\computername
  Opens key
Opens key:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ mountpoints 2 \ cpc \ volume \ \{f90255c2-6bc4-five \ fversion\} \ explorer \ mountpoints \ explorer \
11e3-9fc7-806d6172696f}\
                                     HKCU\software\classes\directory
  Opens key:
                                     HKCR\directory
  Opens key:
                                     HKCU\software\classes\directory\curver
  Opens key:
                                     HKCR\directory\curver
  Opens key:
  Opens key:
                                     HKCR\directory\
                                     HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\explorer\
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\policies\system
  Opens key:
                                     HKCU\software\classes\directory\shellex\iconhandler
  Opens key:
                                     HKCR\directory\shellex\iconhandler
                                     HKCU\software\classes\directory\clsid
  Opens key:
                                     HKCR\directory\clsid
  Opens kev:
  Opens kev:
                                     HKCU\software\classes\folder
  Opens key:
                                     HKCR\folder
                                     HKCU\software\classes\folder\clsid
  Opens key:
  Opens key:
                                     HKCR\folder\clsid
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\explorer
  Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
  Opens key:
                                     HKCU\software\classes\drive\shellex\folderextensions
  Opens key
                                     HKCR\drive\shellex\folderextensions
                                     HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
  Opens key:
4442-804e-409d6c4515e93
Opens key: 409d6c4515e9}
                                     HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\explorer\fileexts
  Opens kev:
                                     HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe
                                     HKCU\software\classes\.exe
  Opens kev:
  Opens key:
                                     HKCR\.exe
  Opens key:
                                     HKCU\software\classes\exefile
  Opens key:
                                     HKCR\exefile
  Opens key:
                                     HKCU\software\classes\exefile\curver
  Opens key:
                                     HKCR\exefile\curver
  Opens key:
                                     HKCR\exefile\
  Opens key:
                                     HKCU\software\classes\exefile\shellex\iconhandler
  Opens key:
                                     HKCR\exefile\shellex\iconhandler
  Opens key:
                                     HKCU\software\classes\systemfileassociations\.exe
  Opens key:
                                     HKCR\systemfileassociations\.exe
  Opens key:
                                     \hbox{\tt HKCU} \\ \hbox{\tt software} \\ \hbox{\tt classes} \\ \hbox{\tt systemfile} \\ \hbox{\tt associations} \\ \hbox{\tt application} \\
  Opens key:
                                     HKCR\systemfileassociations\application
  Opens key:
                                     HKCU\software\classes\exefile\clsid
  Opens key:
                                     HKCR\exefile\clsid
  Opens key:
                                     HKCU\software\classes\*
  Opens key:
                                     HKCR\*
  Opens key:
                                     HKCU\software\classes\*\clsid
                                     HKCR\*\clsid
  Opens kev:
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks
                                     HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-
  Opens kev:
00c04fd91972}\inprocserver32
                                     HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32
  Opens key:
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\policies\associations
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\policies\associations
  Opens key:
                                     HKCU\software\classes\.ade
  Opens key:
                                     HKCR\.ade
  Opens key:
                                     HKCU\software\classes\.adp
  Opens key:
                                     HKCR\.adp
                                     HKCU\software\classes\.app
  Opens kev:
  Opens key:
                                     HKCR\.app
  Opens key:
                                     HKCU\software\classes\.asp
                                     HKCR\.asp
  Opens key:
  Opens key:
                                     HKCU\software\classes\.bas
  Opens key:
                                     HKCR\.bas
   Opens key:
                                     HKCU\software\classes\.bat
  Opens key:
                                     HKCR\.bat
  Opens key:
                                     HKCU\software\classes\.cer
  Opens key:
                                     HKCR\.cer
```

HKCU\software\classes\.chm

```
Opens key:
                                      HKCR\.chm
  Opens key:
                                      HKCU\software\classes\.cmd
  Opens key:
                                     HKCR\.cmd
  Opens key:
                                      HKCU\software\classes\.com
  Opens kev:
                                     HKCR\.com
  Opens kev:
                                      HKCU\software\classes\.cpl
  Opens key:
                                     HKCR\.cpl
  Opens kev:
                                      HKCU\software\classes\.crt
  Opens key:
                                     HKCR\.crt
  Opens kev:
                                      HKCU\software\classes\.csh
  Opens key:
                                      HKCR\.csh
  Opens key:
                                      HKLM\software\microsoft\com3
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clbcatq.dll
  Opens key:
                                      HKLM\software\microsoft\com3\debug
  Opens key
                                      HKLM\software\classes
  Opens key:
                                      HKU\
  Opens key:
                                      HKCR\clsid
  Opens key:
                                      HKCU \setminus software \setminus classes \setminus clsid \setminus \{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4\}
  Opens key:
                                     HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens key:
                                      HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
  Opens key:
                                      HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
  Opens key
                                     HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
                                     HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
  Opens key:
  Opens key
                                     HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserverx86
                                     HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86
  Opens key:
                                     HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
  Opens key:
00c04fb6bfc4}\localserver32
  Opens kev:
                                     HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32
                                     HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
  Opens key
00c04fb6bfc4}\inprochandler32
  Opens key:
                                     HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
  Opens key:
                                     HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandlerx86
                                     HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\nprochandlerx86
  Opens key:
  Opens key
                                     HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\localserver
  Opens key
                                     HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver
  Opens key:
                                     \label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution
options\iertutil.dll
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
  Opens key:
                                      HKCU\software\classes\protocols\name-space handler\
  Opens key
                                     HKCR\protocols\name-space handler
  Opens key:
                                      \label{lem:hkcu} \mbox{HKCU\software\classes\protocols\name-space handler} \\
  Opens key
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings
                                      HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings
  Opens key:
                                     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
                                     HKLM\software\microsoft\internet
  Opens key:
explorer \verb|\main| featurecontrol| feature\_ignore\_policies\_zonemap\_if\_esc\_enabled\_kb918915
  Opens key:
                                     \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zonemap\domains\
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\domains\
                                     \label{lem:hklmsoftware policies microsoft windows \current version \cite{the lement} in terms to the lement of 
  Opens key:
settings\zonemap\ranges\
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zonemap\ranges\
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:
                                      HKLM\software\policies
  Opens key:
                                      HKCU\software\policies
  Opens key:
                                      HKCU\software
  Opens key:
                                     HKLM\software
  Opens key:
                                      \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+internet
settings\zonemap\ranges\
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
```

```
settings\zonemap\protocoldefaults\
    Opens key:
                                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
   Opens key:
                                                                   HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                                                                   HKLM\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\domains\msn.com
                                                                   HKLM\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\domains\msn.com\related
                                                                   HKCU\software\microsoft\internet
   Opens key
explorer\main\featurecontrol\feature use ietldlist for domain determination
   Opens key:
                                                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
                                                                   HKCU\software\microsoft\internet explorer\ietld
    Opens key:
    Opens key:
                                                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
   Opens key:
                                                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
    Opens key:
                                                                   HKCU\software\microsoft\windows\currentversion\internet settings
    Opens key:
                                                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
                                                                   HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_http_username_password_disable
    Opens key:
                                                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
    Opens key:
                                                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
    Opens key:
                                                                   HKLM\software\policies\microsoft\internet explorer
    Opens key:
                                                                   HKLM\software\policies\microsoft\internet explorer\security
                                                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\
    Opens key:
                                                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
    Opens key:
    Opens key:
                                                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
    Opens kev:
                                                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
    Opens kev:
                                                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
    Opens kev:
                                                                   HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
   Opens key:
                                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
   Opens key:
                                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
    Opens key:
                                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
    Opens key:
                                                                   \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\so
settings\zones\0
                                                                   \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
    Opens key:
settings\zones\1
   Opens key:
                                                                   \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\windows\current\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\so
settings\zones\1
   Opens key
                                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
   Opens key:
                                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
   Opens key:
                                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
                                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zones\3
                                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zones\4
   Opens key:
                                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
                                                                   HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_localmachine_lockdown
    Opens key:
                                                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown
                                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
    Opens key
settings\lockdown_zones\
   Opens key:
                                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Opens key
settings\lockdown_zones\
   Opens key:
                                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\lockdown_zones\0
   Opens key
                                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\0
                                                                   HKCU\software\microsoft\windows\currentversion\internet
   Opens key
settings\lockdown zones\1
   Opens key:
                                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\1
   Opens key:
                                                                   \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \normalisation \normalisatio
settings\lockdown_zones\1
                                                                   \label{thm:local_equation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt local_equation} \mbox{\tt local_equation} \mbox{\tt local_equation}} \mbox{\tt local_equation} \mbox{\tt local_
   Opens key:
settings\lockdown_zones\2
   Opens kev:
                                                                   HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
    Opens key:
                                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                                                   HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
settings\lockdown zones\3
    Opens key:
                                                                   \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\3
   Opens key:
                                                                   \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\3
                                                                   HKCU\software\microsoft\windows\currentversion\internet
    Opens key:
```

```
settings\lockdown_zones\4
     Opens key:
                                                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
{\tt settings \lockdown\_zones \label{lockdown} 4}
                                                                                 \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \normalisation \cite{Linear terms} and \cit
     Opens key:
 settings\lockdown_zones\4
                                                                                 HKCU\software\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
     Opens kev:
                                                                                 HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature zones default drive intranet kb941000
      Opens key:
                                                                                 HKCU\software\classes\exefile\shell\open
      Opens key:
                                                                                 HKCR\exefile\shell\open
      Opens key:
                                                                                  HKCU\software\classes\exefile\shell\open\command
                                                                                 HKCR\exefile\shell\open\command
      Opens key:
      Opens key:
\label{thm:culling} \mbox{\current} windows \current version \cites \explorer \cite \cit
      Opens key:
                                                                                 HKLM\software\microsoft\windows\currentversion\app
paths\flashplayer18_a_install.exe
                                                                                 HKCU\software\classes\exefile\shell\open\ddeexec
      Opens kev:
                                                                                 HKCR\exefile\shell\open\ddeexec
      Opens key:
      Opens key:
                                                                                 HKCU\software\classes\applications\flashplayer18_a_install.exe
      Opens key:
                                                                                 HKCR \verb|\applications| flashplayer 18\_a\_install.exe
      Opens key:
                                                                                 HKCU\software\microsoft\windows\shellnoroam
      Opens key:
                                                                                 {\tt HKCU \ } software \verb|\ microsoft \verb|\ windows \verb|\ shell nor oam \verb|\ muicache|
      Opens key:
                                                                                 HKCU\software\microsoft\windows\shellnoroam\muicache\
      Opens key:
                                                                                  HKLM \verb|\software\microsoft\windows\currentversion\explorer\file association
      Opens key:
                                                                                 {\tt HKLM \ } system \verb|\ current control \ } session \ manager \verb|\ appcertdlls \ | \ system \ | 
      Opens key:
                                                                                 {\tt HKLM} \  \  \, \texttt{System} \  \  \, \texttt{Control} \  \  \, \texttt{Session manager} \  \  \, \texttt{appcompatibility}
      Opens key:
                                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
      Opens key:
                                                                                 {\it HKLM\system\wpa\tabletpc}
      Opens key:
                                                                                  HKLM\system\wpa\mediacenter
                                                                                 HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
      Opens key:
      Opens kev:
                                                                                 HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\flashplayer18_a_install.exe
                                                                                 HKLM\software\policies\microsoft\windows\safer\levelobjects
      Opens kev:
      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:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}
      Opens key:
b813f72dbb91}
     Opens key:
7c29ddecae3f3
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
     Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}
      Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
      Opens key:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \begin{tabul
      Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
      Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
      Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus has hes
      Opens key:
HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
     Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
     Opens key
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                                                                                 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
     Opens key:
      Opens key:
                                                                                  HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
      Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
      Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus paths
      Opens key:
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 key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \code ident
      Opens key:
```

```
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus has hes
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
     Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
     Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
     Opens kev:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
     Opens key:
                                                                               \label{thm:linear} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\shell}} \ folders
     Opens key:
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\flashplayer18_a_install.exe
                                                                               HKLM\software\microsoft\windows\currentversion\app paths\install.exe
     Opens key:
     Opens key:
                                                                               HKCU\software\classes\applications\install.exe
     Opens key:
                                                                               HKCR\applications\install.exe
     Opens key
                                                                               HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\install.exe
     Opens key:
                                                                               \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\install.exe
     Opens key
                                                                               \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\winhttp.dll
     Opens key
                                                                               HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens key:
options\msi.dll
     Opens key:
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
     Opens kev:
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msimg32.dll
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens key:
options\winspool.drv
     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\oledlg.dll
     Opens key:
                                                                               HKCU\software\classes\clsid
     Opens key:
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\gdiplus.dll
     Opens key:
                                                                               \label{lem:hklm} \verb+Kklm| software \verb+microsoft| windows nt| current version| image file execution
options\msasn1.dll
     Opens key:
                                                                               \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\crypt32.dll
     Opens key:
                                                                               HKLM \verb|\system| current control set \verb|\services| crypt 32 \verb|\performance| crypt 32 \verb|\performa
     Opens key:
                                                                               \label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{hklm}\software\mbox{$\mbox{microsoft}\windows}$ nt\currentversion\mbox{$\mbox{msasn1}$} \mbox{$\mbox{$\mbox{exp}$}$} \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\m
     Opens key:
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imagehlp.dll
     Opens kev:
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wintrust.dll
     Opens kev:
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mpr.dll
     Opens key:
                                                                               HKLM\system\currentcontrolset\control\networkprovider\hworder
     Opens key:
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp60.dll
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens key:
options\oleacc.dll
     Opens key:
                                                                               HKLM\software\microsoft\ctf\compatibility\install.exe
                                                                               \begin{tabular}{ll} HKLM \end{tabular} is a software \begin{tabular}{ll} is a software \end{tabular} is a software \begin{tabular}{ll} is a software \end{tabular} is a software \begin{tabular}{ll} is a software \end{tabular} is a software \end{tabular} is a software \end{tabular} is a software \begin{tabular}{ll} is a software \end{tabular} is a software \begin{tabula
     Opens key:
options\riched20.dll
     Opens key:
                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\riched32.dll
     Opens key:
                                                                               HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
     Opens key:
                                                                               HKLM\software\microsoft\windows\currentversion\explorer\autocomplete
     Opens key:
                                                                               HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
     Opens key:
                                                                               HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
     Opens key:
                                                                               HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\treatas
     Opens key:
                                                                               HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\treatas
     Opens key
                                                                               HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
     Opens key:
                                                                               HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32
                                                                               HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
     Opens key:
00c04fd7d062}\inprocserverx86
                                                                               HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
     Opens key:
                                                                               HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
     Opens key
00c04fd7d062}\localserver32
                                                                               HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver32
     Opens key:
     Opens key:
                                                                               HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
                                                                               HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler32
     Opens key:
      Opens key:
                                                                               HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandlerx86
     Opens key:
                                                                               HKCR \ clsid \ \{00bb2765-6a77-11d0-a535-00c04fd7d062\} \ inprochandler x 86
                                                                               HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535
     Opens key
00c04fd7d062}\localserver
     Opens key:
                                                                               \label{localserver} HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver. A property of the control 
     Opens key:
                                                                               \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the 
options\browseui.dll
                                                                               HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}
     Opens key:
```

Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383} Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\treatas

Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas Opens key HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprocserver32

HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32 Opens key:

Opens key HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprocserverx86

HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserverx86 Opens kev:

HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-Opens key

00aa005b4383}\localserver32

Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver32

Opens key HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprochandler32

Opens key:  $HKCR \verb|\clsid| \{03c036f1-a186-11d0-824a-00aa005b4383\} \verb|\inprochandler32| \\$ 

Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-

00aa005b4383}\inprochandlerx86

HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandlerx86 Opens key:

Opens key: HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a

00aa005b4383}\localserver

Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}

Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062} Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\treatas

Opens key: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas Opens key HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprocserver32

HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32 Opens key:

HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-Opens key

00c04fd7d062}\inprocserverx86

Opens kev: HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserverx86

HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-Opens key

00c04fd7d062}\localserver32

HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-

00c04fd7d062}\inprochandler32

Opens kev:  $HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler 32$ 

HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-Opens key

00c04fd7d062}\inprochandlerx86

HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86 Opens key:

Opens key HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535

00c04fd7d062}\localserver

Opens key:  $HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver$ Opens key:  $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \policies \network \end{tabular}$ Opens key  $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus comdlg 32$ Opens key:  $HKLM \setminus software \setminus microsoft \setminus ctf \setminus compatibility \setminus flashplayer 18\_a\_install. exe$ Opens key:  $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ 

options\samlib.dll

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

options\wldap32.dll

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

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

options\ntmarta.dll

HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2} Opens key:

HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2} Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-Opens key: 00c04fd705a2}\treatas

Opens key:

HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas Opens key: HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprocserver32

HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32 Opens key:

HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-Opens key

00c04fd705a2}\inprocserverx86

Opens key:  $HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserverx86$ 

Opens key HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\localserver32

Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver32

Opens key HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprochandler32

HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32 Opens kev:

Opens key HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprochandlerx86

Opens key: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx86

HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-Opens key

00c04fd705a2}\localserver

HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver Opens key:

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

options\ieframe.dll

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

Opens key: HKLM\software\microsoft\internet explorer\setup Opens key: HKLM\system\currentcontrolset\control\wmi\security 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} HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc Opens key

00aa00404770}\proxystubclsid32

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

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

00aa004ba90b}\proxystubclsid32

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

```
HKCU\software\classes\interface\{000214e6-0000-0000-c000-
  Opens key:
00000000046}\proxystubclsid32
  Opens key:
                                   HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32
  Opens key:
                                   HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-
00c04f79abd1}\proxystubclsid32
                                   HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32
  Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key
options\flashplayer18_a_install.exe\rpcthreadpoolthrottle
  Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe\rpcthreadpoolthrottle
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe
  Opens key:
Opens key:
                                   HKCU\software\microsoft\internet explorer\main
  Opens key
                                   HKLM\software\microsoft\internet explorer\main
  Opens key:
HKLM \label{lem:hklm} In the limit of the 
1.03
  Opens key
                                   HKLM\software\policies\microsoft\internet explorer\main
  Opens key:
                                   HKCU\software\policies\microsoft\internet explorer\main
  Opens key:
a2ea-08002b30309d}
  Opens key
                                   HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32
  Opens key
                                   HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32
                                   HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
  Opens key
                                   HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}
  Opens key:
                                   HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
  Opens key
08002b30309d}\treatas
                                   HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas
  Opens key:
  Opens key
                                   HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserverx86
                                   HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86
  Opens kev:
                                   HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
  Opens key
08002b30309d}\localserver32
  Opens key:
                                   HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32
  Opens key
                                   HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea
08002b30309d}\inprochandler32
  Opens key:
                                   \label{local-eq:hkcr} $$HKCR\clsid_{871c5380-42a0-1069-a2ea-08002b30309d}\nprochandler32$
                                   HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-
  Opens key
08002b30309d}\inprochandlerx86
                                   HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\nprochandlerx86
  Opens key:
                                   HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea
  Opens key
08002b30309d}\localserver
  Opens key:
                                   HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver
  Opens key
                                   HKCU\software\microsoft\internet
\verb|explorer| \verb|main| featurecontrol| feature\_iedde\_register\_protocol| \\
  Opens key:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_protocol
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\normaliz.dll
  Opens key
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
                                   HKLM\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache
  Opens key
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Opens key
settings\5.0\cache\content
  Opens key:
                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache\content
  Opens key
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key
                                   HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Opens key
settings\5.0\cache\history
  Opens key:
                                   HKLM\software\microsoft\windows\currentversion\internet
HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\cache\extensible cache
  Opens key
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\extensible cache\feedplat
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\extensible cache\iecompat
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
                                   HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\mshist012014033120140407
  Opens kev:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
  Opens key:
                                   HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
                                   HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:
                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:
                                   HKCU\software\microsoft\internet
```

 $explorer \verb|\main\featurecontrol\feature\_bufferbreaking\_818408|$ 

HKLM\software\microsoft\internet

```
explorer\main\featurecontrol\feature_bufferbreaking_818408
                                                 HKCU\software\microsoft\internet
   Opens key:
explorer \verb|\main| featurecontrol| feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954
   Opens key:
                                                 HKLM\software\microsoft\internet
\verb|explorer| main feature control feature skip_post_retry_on_internet write file\_kb895954| feature feature feature from the control feature from t
   Opens kev:
                                                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                                                 HKCU\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\5.0\cache
                                                 HKCU\software\microsoft\internet
   Opens kev:
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
   Opens kev:
                                                 HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_use\_spn\_for\_ntlm\_auth\_disabled| \\
   Opens key:
                                                 HKLM\software\microsoft\internet
\label{lem:control} \begin{tabular}{ll} explorer $$\widehat{m}$ in $$ feature on trol $$ feature use $$ spn_for_ntlm_auth_disabled $$ $$ is $$ for $$ and $$ is $$ for $$ for $$ is $$ for $$ is $$ for $$ fo
                                                 HKCU\software\microsoft\internet
   Opens key:
\verb|explorer\main\featurecontrol\feature_allow_long_international_file names|\\
   Opens key:
                                                 HKLM\software\microsoft\internet
explorer \verb|\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
   Opens key:
                                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback
   Opens kev:
                                                 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 kev:
                                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
   Opens key:
                                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
   Opens key:
                                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
                                                 HKCU\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
   Opens key:
                                                 HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature_passport\_check\_302\_for\_success\_kb949059
   Opens key
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
   Opens key:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
   Opens key:
                                                 HKLM\svstem\currentcontrolset\services\winsock2\parameters
   Opens kev:
HKLM\svstem\currentcontrolset\services\winsock2\parameters\protocol catalog9
   Opens key
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries
   Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 000000000001
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000003
   Opens key:
Opens key:
Opens key:
Opens key:
Opens key
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000000
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000010
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
   Opens key:
HKLM \label{lem:hklm} Which is a substitution of the latest and 
Opens key:
Opens key:
Opens key:
                                                  \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\wpad}} \\
```

HKCU\software\classes\exefile\shell

```
Opens key:
                          HKCR\exefile\shell
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                          HKLM\software\microsoft\windows\currentversion\app paths\msmpeng.exe
 Opens kev:
 Opens key:
                          HKCU\software\classes\applications\msmpeng.exe
                          HKCR\applications\msmpeng.exe
 Opens kev:
                          HKLM\software\policies\microsoft\internet explorer\browseremulation
 Opens key:
                          HKCU\software\policies\microsoft\internet explorer\browseremulation
 Opens kev:
 Opens key:
                          HKCU\software\classes\protocols\name-space handler\res\
 Opens key:
                          HKCR\protocols\name-space handler\res
 Opens key:
                          HKCU\software\classes\protocols\name-space handler\*\
 Opens key:
                          HKCR\protocols\name-space handler\*
 Opens key:
                          HKCU\software\classes\protocols\handler\res
 Opens key:
                          HKCR\protocols\handler\res
 Opens key:
                          HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}
                          HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}
 Opens kev:
                          HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
 Opens key:
00aa00bdce0b}\treatas
                          HKCR \clsid \ \{3050f3bc-98b5-11cf-bb82-00aa00bdce0b\} \treatas
 Opens key:
 Opens key
                          HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
                          HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\tinprocserver32
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
                          HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
 Opens key:
                          HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
 Opens key
00aa00bdce0b}\localserver32
                          HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver32
 Opens key
                          HKLM\software\microsoft\windows
 Opens key:
nt\currentversion\appcompatflags\custom\msmpeng.exe
                          HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
 Opens key
00aa00bdce0b}\inprochandler32
                          HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
 Opens kev:
                          HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82
 Opens key:
00aa00bdce0b}\inprochandlerx86
                          HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\nprochandlerx86
 Opens kev:
 Opens key:
                          HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82
00aa00bdce0b}\localserver
 Opens key:
                          HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msls31.dll
 Opens key:
                          \label{lem:hklm} \verb+Kklm| software \verb+microsoft| windows nt| current version| image file execution
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 \verb|\main| featurecontrol| feature\_css\_data\_respects\_xss\_zone\_setting\_kb912120
 Opens key:
                          HKCU\software\microsoft\internet
explorer \verb|\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
                          HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_aria_support
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_aria_support
                          HKCU\software\microsoft\internet
 Opens key:
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
 Opens key
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_show_hide_events
 Opens key:
                          HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_css\_show\_hide\_events|
 Opens key:
                          HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_display\_node\_advise\_kb833311
                          HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_display_node_advise_kb833311
                          HKCU\software\microsoft\internet
 Opens key
explorer\main\featurecontrol\feature allow expanduri bypass
                          HKLM\software\microsoft\internet
 Opens key
explorer\main\featurecontrol\feature allow expanduri bypass
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\msmpeng.exe
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
                          HKCU\software\microsoft\internet
 Opens kev:
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
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
 Opens key:
                          HKCU\software\microsoft\internet
\verb|explorer| \verb|main| featurecontrol| feature_enable_dynamic_object_caching| \\
                          HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
 Opens key:
```

```
Opens key:
                                     HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
  Opens key:
                                     HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\treatas
  Opens key:
                                     HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\treatas
  Opens kev:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
                                     HKCU\software\microsoft\internet
  Opens kev:
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
  Opens key:
                                     HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprocserver32
                                     Opens key:
  Opens key:
                                     HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprocserverx86
                                     HKCR\clsid\\\{dd313e04-feff-11d1-8ecd-0000f87a470c\\\}\inprocserverx86
  Opens kev:
                                     HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
                                     HKCU\software\microsoft\internet
  Opens key:
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
  Opens key:
                                     HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\localserver32
                                     HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\localserver32
  Opens key:
                                     HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
  Opens key
0000f87a470c}\inprochandler32
                                     HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler32
  Opens key:
                                     HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
  Opens key:
0000f87a470c}\inprochandlerx86
                                     HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandlerx86
  Opens kev:
  Opens key
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
                                    HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
  Opens kev:
0000f87a470c}\localserver
                                     HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\localserver
  Opens key:
  Opens key
                                     \label{lem:hklm} \verb+Kklm/software/microsoft/windows/currentversion/app paths/outlook.exe
  Opens key:
                                     HKLM\software\microsoft\internet explorer\application compatibility
  Opens key:
                                     HKLM\software\policies\microsoft\internet explorer\domstorage
  Opens key:
                                     HKCU\software\policies\microsoft\internet explorer\domstorage
  Opens key:
                                     HKCU\software\microsoft\internet explorer\domstorage
  Opens key:
                                     HKLM\software\microsoft\internet explorer\domstorage
  Opens key:
                                     HKLM\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
                                     HKCU\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
                                     HKCU\software\microsoft\internet explorer\safety\privacie
  Opens key:
                                     HKLM\software\microsoft\internet explorer\safety\privacie
                                     HKLM\software\microsoft\internet explorer\mediatypeclass
  Opens kev:
  Opens kev:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings\accepted documents
                                     HKLM\software\microsoft\windows\currentversion\policies\ratings
  Opens kev:
                                     HKCU\software\microsoft\internet
  Opens key
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
                                     HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
  Opens key:
006097deacf9}
  Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus (5e6ab780-7743-11cf-a12b-microsoft) \setminus
00aa004ae837}
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\settings
  Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cryptui.dll
  Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shdocvw.dll
  Opens key:
                                     HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
                                     HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
  Opens kev:
                                     HKCU\software\classes\protocols\name-space handler\c\
  Opens key:
                                     HKCR\protocols\name-space handler\c
  Opens key:
                                     HKCU\software\classes\protocols\handler\c
  Opens key:
  Opens kev:
                                     HKCR\protocols\handler\c
  Opens key:
                                     HKCU\software\microsoft\internet explorer
                                     HKLM\software\microsoft\internet explorer
  Opens key:
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_mime_handling
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_res_to_lmz
                                     HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_restrict_res_to_lmz
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_load_shdoclc_resources
                                     HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_load_shdoclc_resources
  Opens key:
                                     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_feeds
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_feeds
 Opens key:
                         HKCU\software\classes\protocols\filter\text/html
 Opens kev:
                          HKCR\protocols\filter\text/html
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mpsvc.dll
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature safe bindtoobject
 Opens key:
                         HKLM\software\microsoft\internet
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}
                          HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens key:
00aa00686f13}\treatas
 Opens key:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens key
00aa00686f13}\inprocserver32
 Opens key:
                         HKCR \verb|\clsid|{25336920-03f9-11cf-8fd0-00aa00686f13} \verb|\inprocserver32|
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserverx86
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserverx86
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver32
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver32
 Opens key:
 Opens key:
                          HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprochandler32
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens key:
00aa00686f13}\inprochandlerx86
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandlerx86
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver
 Opens kev:
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
 Opens key:
                          HKLM\system\currentcontrolset\services\tcpip\linkage
 Opens key
                          HKLM\system\currentcontrolset\services\tcpip\parameters\
 Opens key:
                          HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
 Opens key
                          HKLM\system\currentcontrolset\services\netbt\parameters
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_manage_script_circular_refs
                          HKLM\software\microsoft\internet
 Opens key:
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:
                         \label{lem:hklm} \verb+Kklm \+ software + microsoft + internet explorer + security + floppy access
                         HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
 Opens key:
detection
 Opens key:
                         HKLM\software\microsoft\internet explorer\security\adv addrbar spoof
detection
 Opens kev:
                          HKCU\software\classes\protocols\name-space handler\about\
 Opens key:
                          HKCR\protocols\name-space handler\about
 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}
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
 Opens key:
                          HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
 Opens key:
00aa00bdce0b}\treatas
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
 Opens key:
 Opens key
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
 Opens key:
                         HKCR \c1sid \c13050f406-98b5-11cf-bb82-00aa00bdce0b \c1nprocserver32
 Opens key
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
 Opens key:
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
 Opens key:
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32
 Opens kev:
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
 Opens key
00aa00bdce0b}\inprochandler32
 Opens key:
                          HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandler32
 Opens kev
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandlerx86
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
 Opens key:
                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
 Opens key
00aa00bdce0b}\localserver
 Opens key:
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver
 Opens key:
                         HKCU\software\microsoft\internet
```

explorer\main\featurecontrol\feature\_document\_compatible\_mode Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_document\_compatible\_mode

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

Opens key HKLM\software\microsoft\windows\currentversion\internet settings\zones\3

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

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

explorer\main\featurecontrol\feature\_weboc\_document\_zoom Opens key: HKLM\software\microsoft\internet

```
explorer\main\featurecontrol\feature_weboc_document_zoom
  Opens key:
                                           HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\progid
  Opens key:
                                            HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid
                                           Opens kev:
options\msmpeng.exe\rpcthreadpoolthrottle
                                           HKLM\system\currentcontrolset\services\devicesync
  Opens kev:
  Opens kev:
                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
  Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_compat_logging
  Opens key:
                                           HKCU\software\policies\microsoft\internet explorer
  Opens key:
                                            HKCU\software\microsoft\internet explorer\international
  Opens key:
                                            HKLM\software\policies\microsoft\internet explorer\international\scripts
                                            HKCU\software\microsoft\internet explorer\international\scripts
  Opens key:
  Opens key:
                                            HKLM\software\microsoft\internet explorer\international\scripts
                                            HKLM\software\policies\microsoft\internet explorer\settings
  Opens key:
                                            HKCU\software\microsoft\internet explorer\settings
  Opens kev:
  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\currentcontrolset\control\nls\codepage
                                            Opens key:
  Opens key:
                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mlang.dll
                                            HKCU\software\microsoft\windows\currentversion\explorer\travellog
  Opens key:
  Opens key:
                                            HKLM\software\microsoft\windows\currentversion\explorer\travellog
                                            HKLM\software\microsoft\internet explorer\version vector
  Opens key:
                                            HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_zone_elevation
  Opens key:
                                           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
  Opens key:
                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
  Opens key:
                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
  Opens key:
                                           Opens key:
                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature xssfilter
                                           HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_xssfilter
                                            HKCU\software\microsoft\windows\currentversion\internet settings\zones
  Opens key:
                                           HKCU\software\classes\msxml2.domdocument.3.0
  Opens kev:
  Opens key:
                                            HKCR\msxm12.domdocument.3.0
  Opens key:
                                           HKCU\software\classes\msxml2.domdocument.3.0\clsid
  Opens kev:
                                            HKCR\msxml2.domdocument.3.0\clsid
                                           HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}
  Opens kev:
  Opens key:
                                            HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}
  Opens key
                                            HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\treatas
  Opens key:
                                            HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\treatas
  Opens key
                                           HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\inprocserver32
  Opens key:
                                           HKCR \verb|\clsid| \{f5078f32-c551-11d3-89b9-0000f81fe221\} \verb|\inprocserver32| \} | The state of the 
                                            HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
   Opens key:
0000f81fe221}\inprocserverx86
  Opens key:
                                           HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\
  Opens key:
                                           HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9
0000f81fe221}\localserver32
                                           HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\localserver32
  Opens key:
  Opens key:
                                           \label{lem:hkuldefault} $$HKU\.default\software\policies\microsoft\control\ panel\desktop $$
  Opens key
                                           {\it HKU} \verb|\|.default\\| control panel\\| desktop
  Opens key:
                                           HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\inprochandler32
                                           HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandler32
  Opens key:
                                           HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9
  Opens key
0000f81fe221}\inprochandlerx86
                                           HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandlerx86
  Opens key:
                                           HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
  Opens key:
0000f81fe221}\localserver
                                           HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\localserver
  Opens key:
  Opens key:
                                            HKU\.default\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:
                                            HKCR\protocols\name-space handler\
  Opens key:
                                           HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings
                                           HKU\.default\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:
                                           HKU\.default\software\policies\microsoft\internet
explorer\main\featurecontrol
  Opens key:
                                            HKU\.default\software\microsoft\internet explorer\main\featurecontrol
  Opens key:
                                            HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:
                                            HKU \verb|\|.default\| software \verb|\| policies \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet | inte
settings\zonemap\ranges\
  Opens key:
                                           HKU\.default\software\microsoft\internet
\verb|explorer| \verb|main| featurecontrol| feature\_unc\_savedfilecheck| \\
```

```
Opens key:
                         HKU\.default\software\microsoft\windows
nt\currentversion\appcompatflags\layers
 Opens key:
                         HKLM\software\microsoft\windows
\verb|nt\currentversion\appcompatflags\custom\svchost.exe|
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\appcompatflags
 Opens kev:
                          HKCU\software\microsoft\windows nt\currentversion\appcompatflags
                         HKU\.default\software\microsoft\windows nt\currentversion\appcompatflags
 Opens key:
 Opens key:
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\svchost.exe
 Opens key:
options\acgenral.dll
```

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

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

options\shimeng.dll

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

options\msacm32.dll

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

options\userenv.dll

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

Opens key:

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

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msadpcm$ 

Opens key:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \, msg711$ 

Opens key:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ msgsm610$ 

Opens key:  $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} wicrosoft \label{lem:hklm} audio compression manager \label{lem:hklm} driver cache \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hkklm} \label{l$ Opens key  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ ms a cm. ms g723$ 

Opens key

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1

Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet

Opens key: Opens kev:  $HKLM \ \ software \ \ \ icrosoft \ \ \ audio compression manager \ \ \ \ \ \ \ 13 acm$ 

Opens kev: HKLM\system\currentcontrolset\control\mediaresources\acm Opens kev: HKLM\svstem\currentcontrolset\control\productoptions

Opens key: HKU\.default\software\microsoft\windows\currentversion\explorer\user

shell folders

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

Opens key HKU\.default\software\microsoft\windows\currentversion\thememanager

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

Opens key: HKCR\directory\shellex\copyhookhandlers

Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers\cdf

Opens key HKCR\directory\shellex\copyhookhandlers\cdf

Opens key HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-

00c04fd75d13}\inprocserver32

Opens key:  $HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\tinprocserver32$ Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}

Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13} Opens key HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-

00c04fd75d13}\treatas

HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\treatas Opens key: Opens key HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserverx86

HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserverx86 Opens kev:

HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-Opens key

00c04fd75d13}\localserver32

HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\localserver32 Opens key:

Opens key HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-

00c04fd75d13}\inprochandler32

Opens key:  $HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\nprochandler32$ 

Opens key HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-

00c04fd75d13}\inprochandlerx86

HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprochandlerx86 Opens key:

HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-Opens key

00c04fd75d13}\localserver

Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\localserver

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

options\msxml3.dll

Opens key:

HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{67ea19a0-ccef-11d0-8024-00c04fd75d13}

HKCU\software\classes\directorv\shellex\copvhookhandlers\filesvstem Opens kev: Opens key: HKCR\directory\shellex\copyhookhandlers\filesystem HKCU\software\classes\clsid\{217fc9c0-3aea-1069-a2db-

Opens key 08002b30309d}\inprocserver32

HKCR\clsid\{217fc9c0-3aea-1069-a2db-08002b30309d}\inprocserver32 Opens key:  $\label{thm:hkcu} \begin{tabular}{ll} HKCU \software \classes \directory \shellex \copy hook handlers \mbox{\cmments} \\ \end{tabular}$ Opens key:

HKCR\directory\shellex\copyhookhandlers\mydocuments Opens key HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-Opens key

006008059367}\inprocserver32

Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32

Opens key: HKLM\software\microsoft\msxm130

Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}

HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367} Opens key: Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-

006008059367}\treatas

HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-

006008059367}\inprocserverx86

Opens key: 

Opens key HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-

006008059367}\localserver32

Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\localserver32

Opens key HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-

```
006008059367}\inprochandler32
  Opens key:
                                        HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprochandler32
  Opens key
                                        HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-
006008059367}\inprochandlerx86
                                        HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprochandlerx86
  Opens key:
                                        HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-
  Opens key
006008059367}\localserver
  Opens kev:
                                        HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\localserver
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mydocs.dll
  Opens key:
854d-006008059367}
  Opens key:
                                        HKCU\software\classes\directory\shellex\copyhookhandlers\sharing
                                        HKCR\directory\shellex\copyhookhandlers\sharing
  Opens key:
  Opens key:
                                        HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-
00aa003ca9f6}\inprocserver32
                                        HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32
  Opens key:
                                        HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}
  Opens key
  Opens key
                                        HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}
  Opens key:
                                        HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-
00aa003ca9f6}\treatas
  Opens key:
                                        HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\treatas
  Opens key
                                        HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-
00aa003ca9f6}\inprocserverx86
  Opens key:
                                        HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserverx86
  Opens key:
                                        HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-
00aa003ca9f6}\localserver32
                                        HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\localserver32
  Opens key:
                                        HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-
  Opens key:
00aa003ca9f6}\inprochandler32
                                        HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprochandler32
  Opens key:
  Opens key
                                        HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-
00aa003ca9f6}\inprochandlerx86
                                        HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprochandlerx86
  Opens kev:
  Opens key:
                                        HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-
00aa003ca9f6}\localserver
                                        HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\localserver
  Opens kev:
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\atl.dll
  Opens key:
                                        \label{local-observation} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}}
folders
  Opens key
                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntshrui.dll
  Opens key:
a804-00aa003ca9f6}
  Opens key
                                        HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003
  Opens key:
                                        HKLM\software\microsoft\windows nt\currentversion\profilelist
                                        HKLM\software\policies\microsoft\internet
  Opens key
explorer\infodelivery\restrictions
  Opens kev:
                                        HKCU\software\policies\microsoft\internet
explorer\infodeliverv\restrictions
                                        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\
  Opens key:
                                        \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \normalisation \normalisatio
```

settings\zonemap\

Opens key:

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

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

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

f4ceaaf59cfc}\inprocserverx86

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

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

f4ceaaf59cfc}\localserver32

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

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

f4ceaaf59cfc}\inprochandler32

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

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

f4ceaaf59cfc}\inprochandlerx86

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

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

f4ceaaf59cfc}\localserver

HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\localserver Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msimtf.dll

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

Opens key  $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8$ 

 $c9633f71be64 \} \verb|\language| profile$ 

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

c9633f71be64}\languageprofile

```
HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
    Opens key:
c9633f71be64}\languageprofile\0x00000000
    Opens key
                                                                      c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}
    Opens key:
                                                                       HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}
                                                                       HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}
    Opens kev:
    Opens key:
                                                                       HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\treatas
                                                                       HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\treatas
    Opens key:
    Opens key
                                                                      HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32
    Opens key:
                                                                       HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32
                                                                      HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
    Opens key
431b3828ba53}\inprocserverx86
    Opens key
                                                                       HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserverx86
    Opens key:
                                                                       HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83
431b3828ba53}\localserver32
                                                                       HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver32
    Opens key
                                                                       HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
    Opens key
431b3828ba53}\inprochandler32
                                                                       HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53\}\tinprochandler32
     Opens key:
    Opens key
                                                                       HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprochandlerx86
    Opens key:
                                                                      HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprochandlerx86
    Opens key
                                                                       HKCU\software\classes\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\localserver
    Opens key:
                                                                      HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\localserver
                                                                       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
                                                                      HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32
    Opens kev:
                                                                      HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325
    Opens key:
869523e2d6c7}\inprocserverx86
                                                                      HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserverx86
    Opens kev:
    Opens key
                                                                      HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325
869523e2d6c7}\localserver32
     Opens key:
                                                                       HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver 32
                                                                       HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
     Opens key
869523e2d6c7}\inprochandler32
                                                                       \label{local-eq:hkcr} $$ HKCR\clsid_{a4b544a1-438d-4b41-9325-869523e2d6c7} \in \clsid_{a4b544a1-438d-4b41-9325-869523e2d6c7} $$ in prochandler 32 $$ in prochange $$ in procha
    Opens key:
    Opens key
                                                                       HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandlerx86
    Opens key:
                                                                      HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86
    Opens key
                                                                       HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\localserver
    Opens key:
                                                                      HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver
    Opens key:
                                                                       HKLM\software\microsoft\ctf\tip\
                                                                       Opens key:
c9633f71be64}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                      HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
    Opens kev
77e8f3d1aa80}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                      HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
    Opens key:
e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                      HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
    Opens key
                                                                 category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
00c04fc324a1
                                                                       HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
    Opens key
Of816c09f4ee}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
    Opens key:
                                                                       HKCU\software\microsoft\ctf\langbaraddin\
                                                                       HKLM\software\microsoft\ctf\langbaraddin\
     Opens key
                                                                       HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
    Opens key
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 \setminus software \setminus microsoft \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = based \setminus \{c1ee01f2-b3b6-4a6a-9ddb-based \} = based \setminus \{c1ee01f2-b3b6-4a6a-9db-based \} = based \setminus \{c1ee01f2-b3b6-4a6a-9db-based \} = based \setminus \{c1
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
    Opens kev:
Opens key
                                                                      HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                      HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
    Opens key
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                      HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
    Opens key
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                      HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
    Opens key
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                      HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
    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
                                                                       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
                                                                       e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
    Opens key:
                                                                       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
00c04fc324a1 \\ \\ category \\ \\ item \\ \\ a48fa74e-f767-44e4-bfbc-169e8b38ff58 \\ \\ \\
```

 $HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{f89e9e58-bd2f-4008-9ac2-bd2f-4008-9a$ 

```
Of816c09f4ee}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                    HKCU\software\policies\microsoft\internet explorer\control panel
  Opens key:
  Opens key:
                                    \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+internet settings \verb+vurl+ in the latest and the 
history
  Opens kev:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_binary_caller_service_provider
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature binary caller service provider
  Opens key:
                                    HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
  Opens key:
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
                                    HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
  Opens key:
00aa00bbbb58}\treatas
  Opens key:
                                    HKCR \ clsid \ \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \ treat as
                                    HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
  Opens key
00aa00bbbb58}\inprocserver32
  Opens key:
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32
                                    HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
  Opens key:
00aa00bbbb58}\inprocserverx86
  Opens key:
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserverx86
  Opens key
                                    HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1
00aa00bbbb58}\localserver32
  Opens key:
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32
  Opens key:
                                    HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprochandler32
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler32
  Opens key:
                                    HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
  Opens key
00aa00bbbb58}\inprochandlerx86
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandlerx86
  Opens key:
  Opens key
                                    HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver
                                    HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver
  Opens kev:
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jscript.dll
  Opens key:
                                    HKLM\software\microsoft\windows script\features
  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\internet explorer\activex compatibility
  Opens key
                                    HKLM\software\microsoft\internet explorer\activex
compatibility\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
  Opens key:
                                    HKLM\system\currentcontrolset\control\nls\locale
  Opens key:
                                    HKLM \ system \ current controls et \ control \ nls \ locale \ alternate \ sorts
  Opens key
                                    HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:
                                    HKCU \setminus software \setminus classes \setminus appid \setminus flashplayer 18\_a\_install.exe
  Opens key:
                                    HKCR \ appid \ flashplayer 18\_a\_install. exe
  Opens key
                                    HKLM\svstem\currentcontrolset\control\lsa
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine
                                    HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_shim_mshelp_combine
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
  Opens key:
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
  Opens key:
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
  Opens key:
dc030521aabd}\treatas
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas
  Opens key:
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
  Opens key:
dc030521aabd}\inprocserver32
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32
  Opens key:
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
  Opens key
dc030521aabd}\inprocserverx86
  Opens key:
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserverx86
  Opens key
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\localserver32
  Opens key:
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\localserver32
  Opens key
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandler32
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandler32
  Opens kev:
  Opens key
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandlerx86
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandlerx86
  Opens key:
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
  Opens key
dc030521aabd}\localserver
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\localserver
  Opens key:
  Opens key
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dxtrans.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
  Opens key:
                                    HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
                                    HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
  Opens key
  Opens key:
                                    HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a
3c8b00c10000}\treatas
                                    HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\treatas
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32
  Opens key:
                                    \label{local-condition} HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\\\ \label{local-condition} \\ \label{local-condition}
```

Opens key: HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserverx86 Opens key HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-

Opens key

3c8b00c10000}\inprocserverx86

HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-

```
3c8b00c10000}\localserver32
   Opens key:
                                              HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\localserver32
   Opens key
                                              HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandler32
   Opens key:
                                              HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandler32
                                              HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
   Opens key
3c8b00c10000}\inprochandlerx86
                                              HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandlerx86
   Opens kev:
                                              HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
   Opens key
3c8b00c10000}\localserver
   Opens key:
                                              HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\localserver
   Opens key:
                                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
   Opens key:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_behaviors
   Opens key:
                                              HKLM\software\microsoft\internet explorer\default behaviors
                                               HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
   Opens key:
                                               HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}
   Opens kev:
                                               HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
   Opens key:
00c04fd9189d}\treatas
   Opens key:
                                               HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas
   Opens key
                                              HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32
   Opens key:
                                              HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32
   Opens key
                                              HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserverx86
                                              HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserverx86
   Opens key:
   Opens key
                                              HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\localserver32
                                              HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\localserver32
   Opens key:
                                              HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
   Opens key
00c04fd9189d}\inprochandler32
   Opens kev:
                                              HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler32
                                              HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
   Opens key
00c04fd9189d}\inprochandlerx86
   Opens key:
                                              HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\nprochandlerx86
   Opens key:
                                              HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\localserver
   Opens kev:
                                              HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\localserver
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\dciman32.dll
   Opens key:
                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ddraw.dll
   Opens key:
                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ddrawex.dll
   Opens key:
                                               HKLM\hardware\devicemap\video
   Opens key
                                               HKLM\software\microsoft\directdraw\compatibility
   Opens key:
                                               HKLM\software\microsoft\directdraw\compatibility\bug!
   Opens key:
                                               HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus demolition derby 2
   Opens key:
                                               HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus mortal kombat 3
                                               HKLM\software\microsoft\directdraw\compatibility\msgolf98
   Opens kev:
   Opens key:
                                               HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay
   Opens key:
                                               HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo
                                               HKLM\software\microsoft\directdraw\compatibility\rogue squadron
   Opens kev:
                                               HKLM\software\microsoft\directdraw\compatibility\savage
   Opens kev:
   Opens key:
                                               HKLM\software\microsoft\directdraw\compatibility\scorchedplanet
   Opens key:
                                               HKLM\software\microsoft\directdraw\compatibility\silentthunder
                                               HKLM\software\microsoft\directdraw\compatibility\terracide
   Opens key:
   Opens key:
                                               HKLM\software\microsoft\directdraw\compatibility\thirddimension
   Opens key:
\label{thm:limit} \begin{tabular}{ll} HKLM \label{thm:limit} \begin{tabular}{ll} HKLM \label{thm:limit} \begin{tabular}{ll} Software \mbox{$\mathbb{N}$} \begi
   Opens key:
\label{thm:limit} \begin{tabular}{ll} HKLM \label{thm:limit} & \
                                              HKLM\software\microsoft\directdraw\gammacalibrator
   Opens key:
   Opens key:
                                               HKLM\software\microsoft\directdraw
   Opens key:
                                               HKLM\software\microsoft\direct3d
   Opens key:
                                               HKCU \setminus software \setminus classes \setminus clsid \setminus \{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe\}
   Opens key:
                                              HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
   Opens key:
                                              f941e9b7e1fe}\treatas
                                               HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas
   Opens key:
                                              HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
   Opens key
f941e9b7e1fe}\inprocserver32
                                              HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32
   Opens key:
   Opens key:
                                              HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserverx86
                                              HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserverx86
   Opens key:
                                              HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
   Opens key
f941e9b7e1fe}\localserver32
   Opens key:
                                              HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\localserver32
   Opens key:
                                              HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
 f941e9b7e1fe}\inprochandler32
   Opens key:
                                              HKCR\clsid\a7ee7f34-3bd1-427f-9231-f941e9b7e1fe\\\inprochandler32
   Opens key:
                                              HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprochandlerx86
   Opens key:
                                              HKCR\clsid\a7ee7f34-3bd1-427f-9231-f941e9b7e1fe\\\inprochandlerx86
                                              HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
   Opens key:
f941e9b7e1fe}\localserver
   Opens key:
                                              HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\localserver
   Opens key:
                                               HKLM\software\policies\microsoft\internet explorer\dxtrans
   Opens key:
                                               HKCU\software\microsoft\internet explorer\dxtrans
   Opens key:
                                               HKLM\software\microsoft\internet explorer\dxtrans
   Opens key
                                               \label{lem:hkcu} \verb+KKCU\+software\+classes\+dximagetransform.microsoft.gradient
```

HKCR\dximagetransform.microsoft.gradient

```
Opens key:
                                                       HKCU\software\classes\dximagetransform.microsoft.gradient\clsid
    Opens key:
                                                       HKCR\dximagetransform.microsoft.gradient\clsid
                                                       HKCU\software\classes\clsid\\623e2882-fc0e-11d1-9a77-0000f8756a10}
    Opens key:
    Opens key:
                                                       HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}
    Opens key:
                                                       HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-
0000f8756a10}\treatas
    Opens key:
                                                      HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\treatas
                                                       HKLM\software\microsoft\internet explorer\activex
    Opens kev:
compatibility\{623e2882-fc0e-11d1-9a77-0000f8756a10}
                                                      HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-
   Opens key:
0000f8756a10}\inprocserver32
    Opens key:
                                                      HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32
                                                      HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77
    Opens key
0000f8756a10}\inprocserverx86
    Opens key:
                                                      HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\timerocserverx86
    Opens key:
                                                       HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77
0000f8756a10}\localserver32
                                                      HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\localserver32
    Opens kev:
                                                      HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-
    Opens key
0000f8756a10}\inprochandler32
                                                      HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\timerochandler 32
    Opens key:
    Opens key
                                                      HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-
0000f8756a10}\inprochandlerx86
    Opens key:
                                                      HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprochandlerx86
    Opens key
                                                      HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-
0000f8756a10}\localserver
                                                      HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\localserver
    Opens key:
                                                      \label{thm:local_hammon} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\sc mage file execution} \\
    Opens key:
options\svchost.exe\rpcthreadpoolthrottle
   Opens key:
                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winsta.dll
   Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wtsapi32.dll
   Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
    Opens key:
                                                       HKLM\software\microsoft\rpc\securityservice
    Opens key:
                                                       HKLM\system\currentcontrolset\control\securityproviders
    Opens kev:
                                                       HKLM\svstem\currentcontrolset\control\lsa\sspicache
    Opens key:
                                                       HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
    Opens key:
                                                       \label{lem:hklm} \mbox{HKLM} \mbox{$\tt M$} \mbox{$\tt KLM$} \mbox{$\tt M$} \mbox{$\tt Currentversion} \mbox{$\tt image file execution}
options\mswsock.dll
    Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
    Opens key:
                                                       HKLM\system\currentcontrolset\services\winsock\parameters
    Opens key:
                                                       Opens key:
                                                       \label{lem:hklm} \verb+Kklm \system \current control \ lsa \ spicache \ digest. dll
    Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
    Opens key:
                                                       HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
                                                       HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
    Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options\msv1_0.dll
                                                       HKLM\svstem\currentcontrolset\control\session manager\environment
    Opens kev:
                                                       HKU\s-1-5-21-1757981266-507921405-1957994488-1003
    Opens kev:
    Opens key:
                                                       HKU\s-1-5-21-1757981266-507921405-1957994488-1003\environment
                                                       HKU\s-1-5-21-1757981266-507921405-1957994488-1003\volatile environment
    Opens key:
   Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dxtmsft.dll
    Opens key:
                                                       HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}
                                                       HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}
    Opens key:
    Opens key:
                                                       HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-
00c04fd9189d}\treatas
                                                       HKU\s-1-5-21-1757981266-507921405-1957994488-
    Opens key:
1003\software\microsoft\windows nt\currentversion\appcompatflags\layers
    Opens key:
                                                      HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\dllhost.exe
    Opens key:
                                                      HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\treatas
    Opens key:
                                                      HKCU \setminus software \setminus classes \setminus clsid \setminus \{c6365470 - f667 - 11d1 - 9067 - f667 - f
00c04fd9189d}\inprocserver32
                                                      HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\ \ inprocserver 32
    Opens key:
                                                      HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-
    Opens key
00c04fd9189d}\inprocserverx86
                                                      HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserverx86
    Opens key:
    Opens key:
                                                      HKCU \setminus software \setminus classes \setminus clsid \setminus \{c6365470 - f667 - 11d1 - 9067 - f667 - f
00c04fd9189d}\localserver32
                                                      HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\localserver32
    Opens key:
                                                      HKU\s-1-5-21-1757981266-507921405-1957994488-
    Opens key:
1003\software\policies\microsoft\control panel\desktop
    Opens key:
                                                      HKU\s-1-5-21-1757981266-507921405-1957994488-1003\control panel\desktop
   Opens key
                                                      HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-
00c04fd9189d}\inprochandler32
    Opens key:
                                                      HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\\ \ in prochandler 32
    Opens key:
                                                      HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-
00c04fd9189d}\inprochandlerx86
    Opens key:
                                                      HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\ \ in prochandler x 86
                                                       HKU\s-1-5-21-1757981266-507921405-1957994488
    Opens key:
1003\software\microsoft\windows nt\currentversion\appcompatflags
                                                      HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-
    Opens key:
00c04fd9189d}\localserver
    Opens key:
                                                      Opens key:
                                                       HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet settings | leaves the continuous of the continuo
                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{4cb26c03-ff93-11d0-817e-0000f87557db\}
    Opens key
```

HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}

```
Opens key:
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\treatas
  Opens key:
                                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas
  Opens key
                                  HKU\.default\software\policies
  Opens key:
                                  HKU\.default\software
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
  Opens key
0000f87557db}\inprocserver32
                                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32
  Opens kev:
  Opens key
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e
0000f87557db}\inprocserverx86
  Opens key:
                                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserverx86
  Opens key
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\localserver32
  Opens key:
                                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\localserver32
  Opens key
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandler32
  Opens key:
                                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler32
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
  Opens key
0000f87557db}\inprochandlerx86
  Opens key:
                                  HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
  Opens key:
0000f87557db}\localserver
  Opens key:
                                  HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\localserver
  Opens key:
                                  HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:
                                  \label{lem:hkul.default} HKU\.default\software\microsoft\windows\current\version\sline\color{lem:hkul.default\software\microsoft\windows\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\cur
settings\5.0\cache\content
  Opens key
                                  HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
                                  HKCU \setminus software \setminus classes \setminus clsid \setminus \{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd\}
  Opens key:
  Opens key
                                  HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
                                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
                                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Opens key
f4fc1e6ca1bd}\treatas
  Opens key:
                                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas
  Opens key
                                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32
                                  Opens kev:
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
  Opens key:
1003\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
  Opens key:
1003\softwa
                 e\policies\microsoft\windows\safer\codeidentifiers\0\hashes
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
  Opens key
1003\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\softwar
                   \policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\softwa
                    policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
  Opens kev:
1003\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
  Opens key:
1003\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key
                                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserverx86
                                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserverx86
  Opens key:
  Opens key
                                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\localserver32
  Opens key:
                                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\localserver32
                                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Opens key
f4fc1e6ca1bd}\inprochandler32
  Opens key:
                                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler 32
  Opens key
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
                                  HKU\s-1-5-21-1757981266-507921405-1957994488
1003\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
                                  HKU\s-1-5-21-1757981266-507921405-1957994488
1003\software\nolicies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\softwar
                    policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
  Opens key:
1003\softwar
                   .policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
  Opens key:
1003\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key
                                  f4fc1e6ca1bd}\inprochandlerx86
                                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\tinprochandlerx86
  Opens key:
  Opens key
                                  HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\localserver
  Opens key:
                                  HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\localserver
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
  Opens key:
1003\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllhost.exe
  Opens key
                                  HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings\5.0\cache\extensible cache
  Opens key:
                                  HKU\.default\software\microsoft\windows\currentversion\internet
```

settings\5.0\cache\extensible cache\ietld

```
Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sxs.dll
  Opens key:
                                   HKCU\software\classes\typelib
                                   \label{thm:hkul.default} HKU\label{thm:hkul.default} HKU\label{thm:hkul.default} Although the state of the 
  Opens key:
settings\5.0\cache\extensible cache\mshist012013122320131224
                                   HKCR\typelib
  Opens kev:
  Opens key:
                                   HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
                                   HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
  Opens kev:
                                   HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
  Opens key:
                                   HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
  Opens kev:
  Opens key
                                   HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\409
  Opens key:
                                   HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409
  Opens key:
                                   HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\9
  Opens key:
                                   HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9
                                   HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
  Opens key:
00aa003b6061}\1.1\0
                                   HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0
  Opens key:
  Opens key:
                                   HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
00aa003b6061}\1.1\0\win32
                                   HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32
  Opens key:
  Opens key:
                                   HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}
  Opens key
                                   HKCR\typelib\{00020430-0000-0000-c000-00000000046}
                                   HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}\2.0
  Opens key:
                                   HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0
  Opens key
                                   Opens key:
000000000046}\2.0\0
                                   HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0
  Opens key:
                                   HKCU\software\classes\typelib\{00020430-0000-0000-c000-
  Opens key
000000000046}\2.0\0\win32
                                   HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32
  Opens key:
                                   HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
  Opens kev:
  Opens kev:
                                   HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
                                   HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
  Opens kev:
  Opens key:
                                   HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
  Opens key:
                                   HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\409
  Opens kev:
                                   HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\409
                                   HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
  Opens key:
0000f87557db}\1.1\9
                                   HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\9
  Opens key
  Opens key:
                                   HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key
                                   HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\0
  Opens key
                                   HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0
  Opens key:
                                   HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
0000f87557db}\1.1\0\win32
                                   HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32
  Opens key:
                                   HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature disable behaviors draw reentrancy
                                   HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_disable_behaviors_draw_reentrancy
  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:
                                   HKLM\software\policies\microsoft\internet explorer\activities
  Opens key:
                                   HKCU\software\microsoft\internet explorer\activities
                                   HKLM\software\microsoft\internet explorer\activities
  Opens key:
  Opens key:
                                   HKLM\software\policies\microsoft\internet explorer\suggested sites
  Opens key:
                                   HKCU\software\microsoft\internet explorer\suggested sites
  Opens key:
                                   HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}
  Opens key:
                                   HKCR \clsid \ \{0e890f83-5f79-11d1-9043-00c04fd9189d\}
  Opens key:
                                   HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\treatas
                                   HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\treatas
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprocserver32
  Opens key:
                                   HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32
                                   HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
  Opens key
00c04fd9189d}\inprocserverx86
                                   HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserverx86
  Opens key:
  Opens key:
                                   HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\localserver32
                                   HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\localserver32
  Opens key:
                                   HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
  Opens key
00c04fd9189d}\inprochandler32
  Opens key:
                                   HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler32
  Opens key:
                                   HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprochandlerx86
  Opens key:
                                   HKCR \c1sid \end{des} 0e890f83-5f79-11d1-9043-00c04fd9189d \end{des} inprochandler x86
                                   HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
  Opens key
00c04fd9189d}\localserver
  Opens key:
                                   HKU\.default\software\microsoft\windows\currentversion\internet
settings\wpad
  Opens key:
                                   HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\localserver
  Opens key:
                                   HKU\.default\software\microsoft\windows\currentversion\internet
settings\http filters\rpa
  Opens key:
                                   HKLM\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
```

HKLM\software\microsoft\internet

 $\verb|explorer| \verb|main| featurecontrol| feature\_include\_port\_in\_spn\_kb908209|$ 

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasman.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rtutils.dll Opens key: options\tapi32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: HKLM\software\microsoft\windows\currentversion\telephony Opens key: options\rasapi32.dll HKLM\software\microsoft\tracing\rasapi32 Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sensapi.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasadhlp.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dnsapi.dll Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters HKLM\software\policies\microsoft\windows nt\dnsclient Opens key HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key options\dllhost.exe\rpcthreadpoolthrottle Opens key: HKLM\software\microsoft\ctf\compatibility\dllhost.exe Opens key HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider 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 Opens key HKCU\software\microsoft\internet explorer\main\featurecontrol\feature subdownload lockdown Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature subdownload lockdown Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature cross domain redirect mitigation Opens kev: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_cross\_domain\_redirect\_mitigation HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_block\_lmz\_script Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_block\_lmz\_script HKCU\software\microsoft\windows\currentversion\internet settings\user Opens key: agent Opens key: HKCU\software\opera software 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:  $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \begin{tabular}{ll} software \begin{tabular}{ll} microsoft \begin{tabular}{ll} windows \begin{tabular}{ll} constant \begin{tabular}{ll} microsoft \begin{tabular}{ll} windows \begin{tabular}{ll} constant \begin{tabular}{ll} microsoft \begin{tabular}{ll} m$ agent\ua tokens Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\pre platform Opens kev: 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 Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\user agent\post platform Opens key:  $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} internet \end{tabular}$ settings\5.0\user agent\post platform Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\user agent\post platform Opens key:  $\label{thm:linear_loss} \begin{tabular}{ll} HKCU is of tware $$\classes $$ \ttp\shell open command $$ $$ \end{tabular} \label{thm:linear}$ HKCR\http\shell\open\command Opens key Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_scripturl\_mitigation HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature\_scripturl\_mitigation Opens key:  $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} internet settings \end{tabular} winhttp$ Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\connections HKLM\software\microsoft\windows\currentversion\internet Opens key:  $\verb|settings| winhttp \verb| unsafess lapps| \\$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rsaenh.dll Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\connections Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\schannel.dll HKLM\software\policies\microsoft\cryptography Opens key: Opens key: HKLM\software\microsoft\cryptography Opens key: HKLM\software\microsoft\cryptography\offload Opens key: HKCU\software\classes\protocols\name-space handler\file\ Opens key: HKCR\protocols\name-space handler\file Opens key: HKCU\software\classes\.png Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\imgutil.dll Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01} Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01} Opens key HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas Opens key: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas

HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

```
00aa006c1a01}\inprocserver32
   Opens key:
                                              HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\\inprocserver32
   Opens key
                                              HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserverx86
                                              HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86
  Opens key:
                                              HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
   Opens key
00aa006c1a01}\localserver32
                                              HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver32
   Opens kev:
                                              HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
   Opens key:
00aa006c1a01}\inprochandler32
   Opens key:
                                              HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32
  Opens key
                                              HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprochandlerx86
   Opens key:
                                              HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86
   Opens key:
                                              HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\localserver
   Opens key:
                                              HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver
                                              HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
   Opens key
                                              HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
   Opens key
   Opens key:
                                              HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\treatas
   Opens key:
                                              HKCR \clsid \ \{6a01fda0-30df-11d0-b724-00aa006c1a01\} \ \ treat as
   Opens key:
                                              HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
   Opens key:
                                              HKCR \verb|\clsid|{6a01fda0-30df-11d0-b724-00aa006c1a01} \verb|\inprocserver32|
   Opens key
                                              HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserverx86
                                              HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserverx86
   Opens key:
   Opens key:
                                              HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\localserver32
                                              HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32
   Opens key:
                                              HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
   Opens key
00aa006c1a01}\inprochandler32
   Opens kev:
                                              HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32
                                              HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
  Opens key
00aa006c1a01}\inprochandlerx86
   Opens key:
                                              HKCR \verb|\clsid|{6a01fda0-30df-11d0-b724-00aa006c1a01} \verb|\inprochandlerx86| \\
   Opens key
                                              HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\localserver
                                              HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver
   Opens key:
   Opens key
                                              HKCU\software\classes\mime\database\content type
   Opens key
                                              HKCR\mime\database\content type
                                              \label{local-operator} \begin{tabular}{ll} HKCU \software \classes \mbox{$\stackrel{\cdot\cdot}{$}$ mime \database \content type \image/bmp \bits \end{tabular}
   Opens key:
   Opens key:
                                              HKCR\mime\database\content type\image/bmp\bits
   Opens key:
                                              HKCU\software\classes\mime\database\content type\image/gif\bits
   Opens key:
                                              HKCR\mime\database\content type\image/gif\bits
   Opens key:
                                              HKCU\software\classes\mime\database\content type\image/jpeg\bits
   Opens key:
                                              HKCR\mime\database\content type\image/jpeg\bits
   Opens key:
                                              \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \mime \propty \mime \
   Opens key:
                                              HKCR\mime\database\content type\image/pjpeg\bits
   Opens kev:
                                              \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \sime \database \content type \mime \database \content type \sime \database \content type \content type \mime \content type \sime \content type \co
   Opens kev:
                                              HKCR\mime\database\content type\image/png\bits
   Opens key:
                                              HKCU\software\classes\mime\database\content type\image/tiff\bits
                                              HKCR\mime\database\content type\image/tiff\bits
   Opens kev:
                                              HKCU\software\classes\mime\database\content type\image/x-icon\bits
   Opens kev:
   Opens key:
                                              HKCR\mime\database\content type\image/x-icon\bits
   Opens key:
                                              HKCU\software\classes\mime\database\content type\image/x-jg\bits
   Opens key:
                                              HKCR\mime\database\content type\image/x-jg\bits
   Opens key:
                                              HKCU\software\classes\mime\database\content type\image/x-png\bits
   Opens key:
                                              HKCR\mime\database\content type\image/x-png\bits
   Opens key:
                                              HKCU\software\classes\mime\database\content type\image/x-wmf\bits
   Opens key:
                                              HKCR\mime\database\content type\image/x-wmf\bits
   Opens key:
                                              HKCU\software\classes\mime\database\content type\image/x-png
                                              HKCR\mime\database\content type\image/x-png
   Opens key:
   Opens key:
                                              HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
   Opens key:
                                              HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
   Opens key:
                                              HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\treatas
   Opens key:
                                              HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
   Opens key
                                              HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
                                              HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\
   Opens kev:
   Opens key:
                                              HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserverx86
   Opens key:
                                              HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86
                                              HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
   Opens key
00a0c913f750}\localserver32
                                              HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver32
   Opens key:
                                              HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
   Opens key
00a0c913f750}\inprochandler32
   Opens key:
                                              HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32
   Opens key:
                                              HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandlerx86
                                              HKCR\clsid\a3ccedf7-2de2-11d0-86f4-00a0c913f750\\\inprochandlerx86
   Opens kev:
                                              HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4
   Opens key:
00a0c913f750}\localserver
```

Opens key: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver

Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver

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

options\pngfilt.dll

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]

Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

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

Queries value: HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

```
nt\currentversion\gre_initialize[disablemetafiles]
                                    HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\compatibility32[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d631
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\windows[appinit dlls]
                                    HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Oueries value:
  Oueries value:
                                    HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:
                                    HKLM\software\microsoft\ole[rwlockresourcetimeout]
                                     HKCR\interface[interfacehelperdisableall]
  Queries value:
  Queries value:
                                     HKCR\interface[interfacehelperdisableallforole32]
  Queries value:
                                     HKCR\interface[interfacehelperdisabletypelib]
  Queries value:
                                    HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
  Oueries value:
                                    HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableallforole32]
                                     ...
HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
   Queries value:
   Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
   Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Oueries value:
                                     HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 5]
  Queries value:
                                     HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 6]
  Oueries value:
                                     HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 7]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[midil]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Queries value:
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  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\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
   Queries value:
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
   Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
   Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
   Queries value:
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
  Queries value:
                                     HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 7]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Oueries value:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer31
  Oueries value:
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
                                     HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
  Queries value:
  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[mixer9]
  Queries value:
                                     HKCU\control panel\desktop[multiuilanguageid]
   Queries value:
                                     HKCU\control panel\desktop[smoothscroll]
   Queries value:
\label{thm:local_enable_balloontips} \label{thm:local_enable_balloontips} \label{thm:local_enable_balloontips} HKCU \software \mbox{\sc microsoft \windows \current version \explorer \advanced [enableballoontips]]} \label{thm:local_enableballoontips}
                                     HKLM\system\setup[systemsetupinprogress]
   Queries value:
   Queries value:
                                     HKLM\software\microsoft\ctf\systemshared[cuas]
   Queries value:
                                     HKCU\keyboard layout\toggle[language hotkey]
  Oueries value:
                                     HKCU\keyboard layout\toggle[hotkey]
  Oueries value:
                                     HKCU\keyboard layout\toggle[layout hotkey]
  Oueries value:
                                     {\tt HKLM \setminus software \setminus microsoft \setminus ctf[enable anchor context]}
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
  Oueries value:
                                     HKCU\software\microsoft\ctf[disable thread input manager]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ the memanager\+ [compositing]
  Oueries value:
                                     HKCU\control panel\desktop[lamebuttontext]
                                     HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
  Oueries value:
  Oueries value:
                                     HKCU\software\microsoft\windows nt\currentversion\windows[dragde]avl
                                     HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
  Queries value:
                                     HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
  Queries value:
  Queries value:
                                     HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
  Oueries value:
\label{thm:cursoft} \begin{tabular}{ll} HKCU \software \verb|microsoft| windows \verb|currentversion| explorer \verb|advanced[listviewscrollover]| \end{tabular}
  Oueries value:
HKLM \ "software\ "microsoft\ "windows\ "current version\ "explorer\ "advanced\ [list views crollover]" and "microsoft\ "windows\ "current version\ "explorer\ "advanced\ [list views crollover]" and "microsoft\ "windows\ "current version\ "explorer\ "advanced\ [list views crollover]" and "microsoft\ "windows\ "current version\ "explorer\ "advanced\ [list views crollover\ ]" and "microsoft\ "windows\ "explorer\ "advanced\ [list views crollover\ ]" and "microsoft\ "windows\ "explorer\ "advanced\ "explorer\ "explo
\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{thm:linear} list view water mark] \end{tabular}
HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ \ advanced [list viewal phase lect]
  Queries value
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{listviewshadow} \end{tabular}
  Queries value:
Oueries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
```

```
Oueries value:
                                   HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Oueries 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]
  Oueries 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]
  Queries value:
                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
  Queries value:
                                   HKLM\system\wpa\pnp[seed]
  Queries value:
                                   HKLM\system\setup[osloaderpath]
  Oueries value:
                                   HKLM\system\setup[systempartition]
  Oueries value:
                                   HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
  Oueries value:
                                   HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
  Oueries value:
                                   HKLM\software\microsoft\windows\currentversion[devicepath]
  Queries value:
                                   HKLM\software\microsoft\windows\currentversion\setup[loglevel]
  Oueries value:
                                   HKLM\software\microsoft\windows\currentversion\setup[logpath]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
                                   HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Oueries value:
                                   HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[data]
  Oueries value:
11e3-9fc7-806d6172696f}[generation]
  Oueries value:
Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
  Queries value:
Queries value:
\label{thm:local_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \policies \explorer[noactive desktop] \end{tabular}
  Queries value:
\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+policies \verb+explorer[nowebview]
  Oueries value
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
  Oueries value
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
  Oueries value
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                                   HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
  Oueries value:
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
  Queries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{local_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hammon_hamm
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
  Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
  Queries value
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
  Oueries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
  Queries value:
                                   HKCR\directory[docobject]
  Queries value:
                                   HKCR\directory[browseinplace]
                                   HKCR\directory[isshortcut]
  Queries value:
  Queries value:
                                   HKCR\directory[alwaysshowext]
  Queries value:
                                   HKCR\directory[nevershowext]
  Queries value:
                                   HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
  Oueries value:
                                   HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]
  Oueries value:
                                   HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
  Queries value:
Oueries value:
                                   HKCR\.exe[]
                                   HKCR\exefile[docobject]
  Queries value:
  Queries value:
                                   HKCR\exefile[browseinplace]
  Queries value:
                                   HKCR\exefile[isshortcut]
  Queries value:
                                   HKCR\exefile[alwaysshowext]
  Oueries value:
                                   HKCR\exefile[nevershowext]
```

 $\label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\user shell$ 

Queries value:

```
folders[personal]
   Oueries value
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
   Oueries value:
                                                   HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common documents]
                                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Oueries value:
folders[desktop]
                                                   HKLM\software\microsoft\windows\currentversion\explorer\user shell
   Oueries value:
folders[common desktop]
   Oueries value:
                                                   HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
                                                   HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
   Queries value:
00c04fd91972}\inprocserver32[loadwithoutcom]
   Queries value:
                                                   HKCR\.asp[]
   Queries value:
                                                   HKCR\.bat[]
   Queries value:
                                                   HKCR\.cer[]
   Queries value:
                                                   HKCR\.chm[]
   Queries value:
                                                   HKCR\.cmd[]
   Oueries value:
                                                   HKCR\.com[1
                                                   HKCR\.cpl[]
    Queries value:
   Queries value:
                                                   HKCR\.crt[]
   Queries value:
                                                   HKLM\software\microsoft\com3[com+enabled]
   Oueries value:
                                                   HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
   Queries value:
                                                   HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
   Queries value:
                                                   HKLM\software\microsoft\com3[regdbversion]
   Queries value:
                                                   HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
                                                   HKCR \verb|\clsid|{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4} \verb|\inprocserver32[]|
   Queries value:
                                                   HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
   Queries value:
                                                   HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
   Oueries value:
00c04fb6bfc4}\inprocserver32[threadingmodel]
                                                   HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[disableimprovedzonecheck]
   Oueries value:
                                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe]
   Oueries value:
                                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
   Queries value:
                                                   HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
   Oueries value:
                                                   HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
   Oueries value:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
   Queries value:
                                                   {\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet}
settings[createuricachesize]
   Queries value
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
   Queries value:
                                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[enablepunycode]
   Queries value:
                                                   HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
   Oueries value:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
   Oueries value:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\2[flags]
                                                   HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\zones\3[flags]
   Queries value:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
                                                   HKCU\software\microsoft\internet
   Queries value:
explorer \verb|\main| feature metric metric
   Queries value:
                                                   HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
   Queries value:
                                                   HKLM\software\microsoft\internet
explorer \verb|\main| feature metric metric
   Queries value:
                                                   HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                                                   \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Queries value:
settings[specialfolderscachesize]
   Queries value:
                                                   \label{lem:hklm} \verb+ HKLM \+ software \+ icrosoft \+ windows \+ current version \+ internet
settings[specialfolderscachesize]
   Oueries value:
                                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
   Queries value:
                                                   HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
   Queries value:
                                                   HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1806]
                                                   HKCR\exefile\shell\open\command[]
   Queries value:
   Queries value:
                                                   HKCR\exefile\shell\open\command[command]
                                                   HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
   Queries value:
   Queries value:
                                                   HKCU\software\microsoft\windows\shellnoroam\muicache[c:\program
files\flashplayer18_a_install.exe]
   Queries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \mbox{$\operatorname{microsoft}$ windows \current version \explorer \file association [cutlist] \end{substitute}
   Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
   Queries value:
Queries value:
manager\appcompatibility[disableappcompat]
```

Queries value:

HKLM\system\wpa\mediacenter[installed]

Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834dbe2efd2c1a33}[itemdata] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834dbe2efd2c1a33}[saferflags] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[itemdata] Queries value: edd5fbde1328}[hashalg] Queries value: edd5fbde1328}[itemsize]  $HKLM \label{lem:hklm} Which is the like of the like$ edd5fbde1328}[saferflags] Oueries value: b813f72dbb91}[itemdata] Queries value: b813f72dbb91}[hashalg] Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91}[itemsize] Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91}[saferflags] Oueries value: 7c29ddecae3f}[itemdata] Oueries value: 7c29ddecae3f}[hashalg] 7c29ddecae3f}[itemsize] Queries value 7c29ddecae3f}[saferflags] Queries value: 085bcc18a68d}[itemdata] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[hashalg] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemsize] Oueries value: 085bcc18a68d}[saferflags] Queries value: b91490411bfc}[itemdata] Queries value: b91490411bfc}[hashalg] Queries value b91490411bfc}[itemsize] Queries value: b91490411bfc}[saferflags] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename] HKLM\software\microsoft\windows\currentversion\app Queries value: paths\install.exe[runascommand] Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\program files\install.exe] HKLM\software\microsoft\windows\currentversion\app Queries value: paths\install.exe[useshortname] Oueries value: HKLM\software\microsoft\windows\currentversion\app paths\install.exe[appendpath] Queries value: HKLM\software\microsoft\windows\currentversion\app paths\install.exe[path]

paths\install.exe[runascommand]
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[c:\program files\install.exe]
Queries value: HKLM\software\microsoft\windows\currentversion\app paths\install.exe[useshortname]
Queries value: HKLM\software\microsoft\windows\currentversion\app paths\install.exe[appendpath]
Queries value: HKLM\software\microsoft\windows\currentversion\app paths\install.exe[path]
Queries value: HKLM\software\microsoft\windows\currentversion\app paths\install.exe[runasonnonadmininstall]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\install.exe[debugger]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\install.exe[executeoptions]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\install.exe[executeoptions]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\install.exe[executeoptions]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\install.exe[executeoptions]

```
options\install.exe[disableheaplookaside]
                                                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
      Oueries value:
options\install.exe[shutdownflags]
      Oueries value:
                                                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe[minimumstackcommitinbytes]
                                                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
      Oueries value:
options\install.exe[globalflag]
                                                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
      Oueries value:
options\install.exe[debugprocessheaponly]
                                                                                           HKLM\software\microsoft\windows
      Oueries value:
nt\currentversion\compatibility32[flashplayer18_a_install]
                                                                                           HKLM\software\microsoft\windows nt\currentversion\ime
      Queries value:
compatibility[flashplayer18 a install]
                                                                                           \label{thm:local_hammon} \mbox{HKLM\software\mbox{\sc microsoft\windows} nt\current version\sc mage file execution} \\
      Queries value:
options\install.exe[applicationgoo]
      Queries value:
                                                                                           HKLM\software\microsoft\windows
nt\currentversion\compatibility32[install]
      Oueries value:
                                                                                           HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[install]
      Queries value
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
      Oueries value
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus autocomplete [autosuggest]
      Oueries value
HKCU \ software \ microsoft \ windows \ current version \ (explorer \ autocomplete [always use tab]) \ and \ an arrange \ (explorer) \ and \ (ex
      Queries value:
                                                                                           HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
      Queries value:
                                                                                           HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
                                                                                           \label{local-equation} \mbox{HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062\}[appid]}}
      Queries value:
                                                                                           HKCR\clsid\{00bb2765-6a77-11d0-a535-
      Oueries value:
00c04fd7d062}\inprocserver32[threadingmodel]
                                                                                         HKCR\clsid\{03c036f1-a186-11d0-824a-
      Queries value:
00aa005b4383}\inprocserver32[inprocserver32]
                                                                                           HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]
      Oueries value:
                                                                                           HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[appid]
      Oueries value:
                                                                                          HKCR\clsid\{03c036f1-a186-11d0-824a-
      Queries value:
00aa005b4383}\inprocserver32[threadingmodel]
      Oueries value:
                                                                                          HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
                                                                                           HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
      Queries value:
                                                                                           HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062\}[appid]\\
      Queries value:
                                                                                           HKCR\clsid\{00bb2763-6a77-11d0-a535-
      Queries value:
00c04fd7d062}\inprocserver32[threadingmodel]
                                                                                           HKCU\software\microsoft\windows\currentversion\policies\explorer[norun]
      Queries value:
      Queries value:
\label{local-objective} HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [nodrives]
      Queries value
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonectdisconnect]
      Oueries value
HKCU\software\microsoft\windows\currentversion\policies\explorer[norecentdocshistory]
      Oueries value
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[alwaysdropup]
      Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noclose]
                                                                                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
      Oueries value:
 folders[local appdata]
      Queries value:
                                                                                           HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
                                                                                           HKCR\clsid\{8856f961-340a-11d0-a96b-
      Queries value:
00c04fd705a2}\inprocserver32[inprocserver32]
                                                                                           HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
      Queries value:
                                                                                           HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[appid]
      Queries value:
      Queries value:
                                                                                           HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
      Queries value:
                                                                                           HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
       Queries value:
                                                                                           \label{thm:local_explore} \begin{tabular}{ll} HKLM \label{thm:local_explore} In the constant of the constant
      Queries value:
                                                                                           HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
      Oueries value
                                                                                           ab78-1084642581fb]
      Queries value:
                                                                                           0000-00000000000001
      Oueries value:
                                                                                           HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
                                                                                           HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
      Queries value:
      Oueries value:
                                                                                           HKLM\software\microsoft\internet explorer\setup[installstarted]
                                                                                           HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
      Oueries value:
                                                                                           HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
      Queries value:
                                                                                           HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[]
      Queries value:
                                                                                           HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32[]
      Queries value:
                                                                                           HKLM\software\microsoft\internet
      Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[flashplayer18_a_install.exe]
      Oueries value:
HKLM \label{lem:hklm} In the limit of the 
      Oueries value:
HKLM \label{lem:hklm} In the limit of the 
      Queries value:
HKLM \label{lem:hklm} In the latest and the lates
      Queries value
HKLM \label{lem:hklm} Which is the like the li
      Queries value:
HKLM \ software \ `microsoft\ `windows \ `current version \ 'shell compatibility \ `applications \ 'install.exe[win95defview] \ install.exe[win95defview] \ install.exe[
      Queries value:
```

```
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ install. exe[docobject]
        Oueries value
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus shell compatibility \setminus applications \setminus install.exe[flushnowaitalways]
        Oueries value:
HKLM \ software \ `microsoft \ 'windows \ 'current version's hell compatibility \ 'applications \ 'install.exe[mycomputerfirst]' and the sum of the sum 
        Oueries value
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ install. exe[oldregitemgdn] \ details \
       Oueries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[loadcolumnhandler]
        Oueries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[ansi]
       Queries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lklm} \labell} \label{lklm} \labell} \label{lklm} \labell{lklm} \
        Queries value:
HKLM \label{lem:hklm} Which is the like of the like 
        Queries value:
HKLM \label{lem:hklm} Which is the like of the like 
        Oueries value:
                                                                                                              HKCU\software\microsoft\internet explorer\main[frametabwindow]
                                                                                                              HKLM\software\microsoft\internet explorer\main[frametabwindow]
         Queries value:
        Queries value:
                                                                                                              HKCU\software\microsoft\internet explorer\main[framemerging]
         Queries value:
                                                                                                              HKLM\software\microsoft\internet explorer\main[framemerging]
        Oueries value:
                                                                                                             HKCU\software\microsoft\internet explorer\main[sessionmerging]
        Oueries value:
                                                                                                             HKLM\software\microsoft\internet explorer\main[sessionmerging]
        Oueries value:
HKLM \label{lem:hklm} Which is a point of the content of the con
        Oueries value:
HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{lem:h
        Oueries value
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ install. exe[ignore enumre set] \ make the compatibility \ applications \ make the compatibility \ applicatio
       Queries value:
HK\dot{L}M\ software \ microsoft\ windows \ current version\ shell compatibility\ applications\ install.\ exe[ansidisplaynames]
       Queries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[fileopenbogusctrlid]
       Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ install. exe[forcelfnidlist]
       Queries value:
HKLM \label{lem:hklm} In the limit of the 
1.03[requiredfile]
        Oueries value:
                                                                                                              HKCU\software\microsoft\internet explorer\main[admintabprocs]
                                                                                                              HKLM\software\microsoft\internet explorer\main[admintabprocs]
         Queries value:
        Queries value:
                                                                                                              HKLM\software\policies\microsoft\internet explorer\main[tabprocgrowth]
         Queries value:
                                                                                                              HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
                                                                                                              {\tt HKLM \setminus software \setminus microsoft \setminus internet \ explorer \setminus main[tabprocgrowth]}
        Queries value:
                                                                                                              HKLM\software\microsoft\internet explorer\main[navigationdelay]
         Queries value:
        Queries value:
                                                                                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
        Queries value:
                                                                                                             HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[loadwithoutcom]
        Queries value:
                                                                                                             HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
       Oueries value:
                                                                                                             HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
        Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]
                                                                                                             HKLM\software\microsoft\windows\currentversion\shell
       Oueries value:
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0x401]
       Queries value:
                                                                                                             HKCU\software\microsoft\windows\currentversion\shell
0x4011
                                                                                                             HKCR\clsid\{871c5380-42a0-1069-a2ea-
        Queries value:
08002b30309d}\inprocserver32[inprocserver32]
        Queries value:
                                                                                                             HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
                                                                                                              HKCR\clsid\{871c5380-42a0-1069-a2ea-
         Queries value
08002b30309d}\inprocserver32[threadingmodel]
        Queries value:
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
 settings[fromcachetimeout]
                                                                                                              HKCU\software\microsoft\windows\currentversion\internet
        Queries value:
settings[secureprotocols]
        Queries value:
                                                                                                             HKLM\software\policies\microsoft\internet
explorer\main[security_hklm_only]
        Oueries value:
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
       Queries value:
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
       Queries value:
                                                                                                              HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
       Queries value:
settings[idnenabled]
                                                                                                              HKCU\software\microsoft\windows\currentversion\internet
       Queries value:
settings[cachemode]
                                                                                                              HKCU\software\microsoft\windows\currentversion\internet
       Queries value:
settings[enablehttp1_1]
       Queries value:
                                                                                                              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
        Queries value
                                                                                                              HKCU\software\microsoft\windows\currentversion\internet
 settings[enablenegotiate]
                                                                                                             \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
        Queries value:
 settings[disablebasicoverclearchannel]
                                                                                                             HKCU\software\microsoft\internet
        Queries value
 explorer\main\featurecontrol[feature_clientauthcertfilter]
        Queries value:
                                                                                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
        Oueries value:
                                                                                                             HKCU\software\microsoft\windows\currentversion\internet
```

settings[clientauthbuiltinui]

```
Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
{\tt settings \ 1.0 \ cache[sessions tart time default deltasecs]}
 Oueries 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]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\content[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\cookies[peruseritem]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
 Queries value:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache\history[peruseritem]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[peruseritem]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\history[cachelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
 Oueries value
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
 Queries value
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value
settings\5.0\cache\extensible cache\feedplat[cachepath]
 Queries value
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
 Queries value
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries 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]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
 Oueries value
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
 Queries value
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries 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]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
```

 $settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|privacie:[cacherepair]|$ 

```
HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
 Queries value
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablereadrange]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxhttpredirects]
  Queries value:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[maxconnectionsperserver]
                           \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
{\tt settings[maxconnectionsperserver]}
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1 Oserver]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperproxy]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connecttimeout]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:
                           \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[connectretries]
  Queries value
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+internet
settings[receivetimeout]
 Oueries value:
                           \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings[receivetimeout]
 Queries value
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[scavengecachelowerbound]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[certcachenovalidate]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Queries value
                           HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                           HKLM\software\microsoft\internet
  Queries value
explorer\main\featurecontrol\feature_protocol_lockdown[install.exe]
  Queries value:
                           HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature_disable_unicode_handle_closing_callback[flashplayer18\_a_install.exe]|
  Oueries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback[*1
 Queries value:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
{\tt settings[disable caching of sslpages]}
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[leashlegacycookies]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablent4rascheck]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
  Queries value:
                           \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[dialupuselansettings]
  Queries value
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[bypassftptimecheck]
                           HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
  Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
  Oueries value:
                           HKLM\software\microsoft\windows\currentversion\internet
{\tt settings[releases ocket during 401 auth]}
```

```
\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings[wpadsearchalldomains]
  Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
 Queries value
                             HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
 Oueries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
 Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                             HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
 Queries value:
                             {\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet}
settings[enablehttptrace]
                             \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[nocheckautodialoverride]
  Queries value:
                             HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                              HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[dontusednsloadbalancing]
  Queries value:
                              HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                              \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings[sharecredswithwinhttp]
 Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
{\tt settings[mimeexclusionlistforcache]}
 Queries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
                             HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscacheenabled]
 Oueries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
                             \label{thm:local_hammon_hammon} \verb+HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscachetimeout]
                              HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpost]
  Oueries value:
                              HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Queries value:
                              \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[warnonzonecrossing]
  Queries value:
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcer
                           ending]
                              HKCU\sc
  Queries value:
                                        tware\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[warnonpostredirect]
 Queries value:
                             \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings[alwaysdrainonredirect]
 Queries value
                             HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[num catalog entries]
  Queries value:
Queries value:
Queries value:
Queries value
Queries value
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
Queries value:
                              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown[install.exe]
                             HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature localmachine lockdown[install.exe]
  Queries value:
Queries value:
HKLM \label{lem:hklm} Which is a substitution of the latest and 
  Queries value:
Queries value
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 [serial\_access\_num]
Queries value
HKLM \ system \ current controls et \ services \ win sock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 00000000001 [library path]
  Oueries value
```

Oueries value:  $HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ \ 000000000001 [providerid]$ 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\00000000001[supportednamespace] Oueries value:  $HKLM \ system \ \ current control set \ services \ \ winsock 2 \ parameters \ \ namespace\_catalog5 \ \ catalog\_entries \ \ \ 000000000001 \ [enabled]$ Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[version] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[storesserviceclassinfo] Queries value: Queries value: Oueries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ (catalog\_entries \ 0000000000002 [providerid]) \ details a simple of the system \ details and the system \ details a simple of the sy$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily] Queries value: Queries value: Queries value  $HKLM \ system \ \ current controls et \ services \ \ winsock 2 \ parameters \ \ namespace\_catalog5 \ \ catalog\_entries \ \ \ 0000000000002 \ [version]$ Queries value:  $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries \ 00000000000002 \ [storesserviceclass info]$ Oueries value: Queries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003fproviderid Queries value:  $HKLM \label{lem:hklm} Which is the property of the property$ Queries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[enabled] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[version] Queries value Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters [ws 2\_32 numhandle buckets]$ Queries value HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32spincount] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline] Oueries value: HKCR\exefile\shell[1 Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[enableautodial] HKLM\software\microsoft\windows\currentversion\internet Oueries value: settings[urlencoding] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[truncatefilename] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[badproxyexpirestime] Queries value:  $\label{thm:linear_hat} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \policies \explorer [nofilemenu] \end{tabular} \label{thm:linear_hat}$ Queries value:  $HKCU\software\microsoft\windows\shellnoroam\muicache[c:\docume~1\admin\locals~1\temp\rarsfx0\msmpeng.exe]$ HKCR\protocols\handler\res[clsid] Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-Queries value: 00aa00bdce0b}\inprocserver32[inprocserver32] Queries value:  $HKCR \verb|\clsid|{3050f3bc-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprocserver32[]|$ HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}[appid] Oueries value: Oueries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[threadingmodel] Oueries value: HKLM\software\microsoft\internet  $explorer \verb|\main\feature_legacy_dispparams[flashplayer18\_a\_install.exe]|$ Queries value: HKLM\software\microsoft\internet  $\verb|explorer\main\featurecontrol\feature_legacy_dispparams[*]|$ Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_object\_caching[flashplayer18\_a\_install.exe] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature object caching[\*] HKCR\clsid\{dd313e04-feff-11d1-8ecd-Queries value: 0000f87a470c}\inprocserver32[inprocserver32] Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[] Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}[appid] Oueries value: HKLM\software\microsoft\internet explorer\application compatibility[flashplayer18\_a\_install.exe] Queries value: HKCU\software\microsoft\internet explorer\domstorage[totallimit] Queries value: HKCU\software\microsoft\internet explorer\domstorage[domainlimit]

Queries value: HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd0000f87a470c}\inprocserver32[threadingmodel]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\\{75048700-ef1f-11d0-9888006097deacf9}[version]

```
Oueries value:
00aa004ae837}[version]
   Oueries value:
                                             HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown[flashplayer18 a install.exel
   Oueries value:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown[flashplayer18 a install.exe]
   Oueries value:
                                             HKCU\software\microsoft\internet explorer[no3dborder]
                                             HKLM\software\microsoft\internet explorer[no3dborder]
   Oueries value:
   Oueries value:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[flashplayer18_a_install.exe]
   Queries value:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
   Queries value:
\label{thm:local_hammon} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| policies \verb|\explorer[noinstrumentation]| \\ \end{tabular}
   Queries value:
HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ user as sist \ \{75048700-ef1f-11d0-9888-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-198860-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-19886-
006097deacf9}\count[hrzr_pgyfrffvba]
   Queries value:
HKCU \setminus software \setminus irrestable for all the first of the f
00aa004ae837}\count[hrzr_pgyfrffvba]
   Queries value:
                                             HKLM\software\microsoft\ole[maximumallowedallocationsize]
   Oueries value:
                                             HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_mime\_sniffing[flashplayer18\_a\_install.exe]|
   Queries value:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing[*]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[istextplainhonored]
                                             HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature feeds[flashplayer18 a install.exe]
                                             HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature feeds[*]
                                             HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\compatibility32[msmpeng]
                                             HKLM\software\microsoft\windows nt\currentversion\ime
   Oueries value:
compatibility[msmpeng]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
   Oueries value:
                                             HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_safe\_bindtoobject[flashplayer18\_a\_install.exe]|
   Queries value:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
   Queries value:
                                             HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[inprocserver32]
   Queries value:
                                             HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\nprocserver32[]
   Queries value:
                                             HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid]
   Oueries value:
                                             HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[threadingmodel]
   Oueries value:
                                             HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinset]
   Oueries value:
                                             HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrolldelay]
   Oueries value:
                                             HKCU\software\microsoft\windows
nt\currentversion\windows[dragscrollinterval]
                                             HKLM\software\microsoft\internet
   Oueries value:
explorer\main\featurecontrol\feature_restrict_filedownload[flashplayer18_a_install.exe]
                                             HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_restrict_filedownload[*]
   Queries value:
                                             HKCR\protocols\handler\about[clsid]
   Queries value:
                                             HKCR\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
                                             \label{local-bb82-00aa00bdce0b} Linprocserver 32[] \\
   Queries value:
                                              HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid]
   Queries value:
                                             HKCR\clsid\{3050f406-98b5-11cf-bb82-
   Queries value:
00aa00bdce0b}\inprocserver32[threadingmodel]
   Queries value:
                                             HKLM\software\microsoft\internet explorer\registration[productid]
   Oueries value:
                                             \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ 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]
   Oueries value:
                                              HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
                                              HKLM\software\policies\microsoft\internet explorer[smartdithering]
   Oueries value:
                                              HKCU\software\microsoft\internet explorer[smartdithering]
   Oueries value:
                                              HKCU\software\microsoft\internet explorer[rtfconverterflags]
   Oueries value:
                                              HKLM\software\policies\microsoft\internet explorer\main[usecleartype]
   Oueries value:
                                              HKCU\software\microsoft\internet explorer\main[usecleartype]
   Queries value:
                                             HKLM\software\policies\microsoft\internet
   Queries value:
explorer\main[page_transitions]
   Queries value:
                                             HKCU\software\microsoft\internet explorer\main[page_transitions]
   Queries value:
                                             HKLM\software\policies\microsoft\internet
explorer\main[use_dlgbox_colors]
   Queries value:
                                              HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors]
                                             HKLM\software\policies\microsoft\internet explorer\main[anchor
   Oueries value:
underline]
   Queries value:
                                              HKCU\software\microsoft\internet explorer\main[anchor underline]
   Queries value:
                                              HKCU\software\microsoft\internet explorer\main[css_compat]
   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 \setminus software \setminus policies \setminus microsoft \setminus internet \ explorer \setminus main[display \ inline]
```

HKCU\software\microsoft\internet explorer\main[display inline videos]

videos]
Queries value:

```
Oueries value:
                                    HKLM\software\policies\microsoft\internet
explorer\main[play_background_sounds]
  Oueries value:
                                    \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\internet explorer\mbox{\tt main[play\_background\_sounds]}}
                                    HKLM\software\policies\microsoft\internet explorer\main[play_animations]
HKCU\software\microsoft\internet explorer\main[play_animations]
  Queries value:
  Oueries value:
                                    HKLM\software\policies\microsoft\internet
  Oueries value:
explorer\main[print_background]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\main[print background]
                                    HKCU\software\microsoft\internet explorer\main[use stylesheets]
  Oueries value:
  Oueries value:
                                    HKLM\software\policies\microsoft\internet explorer\main[smoothscroll1]
  Queries 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]
  Queries value:
                                    HKLM\software\policies\microsoft\internet explorer\main[show image
placeholders]
  Queries value:
                                    HKCU\software\microsoft\internet explorer\main[show image placeholders]
  Oueries value:
                                    HKLM\software\policies\microsoft\internet explorer\main[disable script
debugger1
   Queries value:
                                    HKCU\software\microsoft\internet explorer\main[disable script debugger]
  Queries value:
                                    HKCU\software\microsoft\internet explorer\main[disablescriptdebuggerie]
   Queries value:
                                    HKCU\software\microsoft\internet explorer\main[move system caret]
  Oueries value:
                                    \label{lem:hkcu} \verb+KKCU\software\microsoft\internet explorer\main[force offscreen]
composition]
  Oueries value:
                                    HKLM\software\policies\microsoft\internet explorer\main[enable
autoimageresize]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\main[enable autoimageresize]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\main[usethemes]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\main[usehr]
                                    HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus main[q300829]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\main[cleanup htcs]
  Oueries value:
                                    HKLM\software\policies\microsoft\internet explorer\main[xdomainrequest]
  Queries value:
                                    HKCU\software\microsoft\internet explorer\main[xdomainrequest]
  Queries value:
                                    HKLM\software\microsoft\internet explorer\main[xdomainrequest]
  Oueries value:
  Queries value:
                                    HKLM\software\policies\microsoft\internet explorer\main[domstorage]
  Queries value:
                                    HKCU\software\microsoft\internet explorer\main[domstorage]
  Queries value:
                                    HKLM\software\microsoft\internet explorer\main[domstorage]
  Oueries value:
                                    HKCU\software\microsoft\internet
explorer\international[default_codepage]
   Oueries value:
                                    HKCU\software\microsoft\internet explorer\international[autodetect]
                                    HKCU\software\microsoft\internet
   Queries value:
explorer\international\scripts[default iefontsizeprivate]
   Queries value:
                                    HKCU\software\microsoft\internet explorer\settings[anchor color]
                                    HKCU\software\microsoft\internet explorer\settings[anchor color visited]
   Queries value:
  Queries value:
                                    HKCU\software\microsoft\internet explorer\settings[anchor color hover]
  Queries value:
                                    HKCU\software\microsoft\internet explorer\settings[always use my colors]
  Queries value:
                                    HKCU\software\microsoft\internet explorer\settings[always use my font
size]
  Queries value:
                                    HKCU\software\microsoft\internet explorer\settings[always use my font
face]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\settings[disable visited
hyperlinks]
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\settings[use anchor hover
color1
  Oueries value:
                                    HKCU\software\microsoft\internet explorer\settings[miscflags]
                                    HKCU\software\microsoft\windows\currentversion\policies[allow
  Oueries value:
programmatic cut_copy_paste]
  Queries value:
                                    HKLM\system\currentcontrolset\control\nls\codepage[950]
                                    HKCU\software\microsoft\internet
  Queries value:
explorer\international\scripts\3[iefontsize]
  Queries value:
                                    HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsizeprivate]
  Queries value:
                                    HKCU\software\microsoft\internet
explorer\international\scripts\3[iepropfontname]
                                    HKCU\software\microsoft\internet
  Queries value:
explorer\international\scripts\3[iefixedfontname]
  Queries value:
                                    HKCU\software\microsoft\internet explorer\international[acceptlanguage]
   Oueries value:
                                    HKLM\software\microsoft\internet explorer\version vector[vml]
  Oueries value:
                                    HKLM\software\microsoft\internet explorer\version vector[ie]
  Oueries value:
                                    HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_zone\_elevation[flashplayer18\_a\_install.exe]|
  Oueries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[*]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[2700]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\0[2700]
                                    HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_xssfilter[flashplayer18_a_install.exe]
                                    HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature_xssfilter[*]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\zones[securitysafe]
  Queries value:
                                    HKCR\msxml2.domdocument.3.0\clsid[]
                                    HKCR\clsid\{f5078f32-c551-11d3-89b9-
  Oueries value:
0000f81fe221}\inprocserver32[inprocserver32]
   Queries value:
                                    HKU\.default\control panel\desktop[multiuilanguageid]
  Queries value:
                                    \label{lem:hkcrclsid} $$ HKCR\clsid_{f5078f32-c551-11d3-89b9-0000f81fe221} \in $$ 21_{c5078f32-c551-11d3-89b9-0000f81fe221} $$ 21_{c5078f32-c551-11d3-89b9-0000f81fe221} = $$ 21_{c5076f32-c551-11d3-89b9-0000f81fe221} = $$ 21_{c5076f32-c551-11d3-89b9-0000f81fe22
   Oueries value:
                                    HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}[appid]
  Queries value:
                                    HKCR\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\inprocserver32[threadingmodel]
   Queries value:
                                    HKU\.default\control panel\desktop[smoothscroll]
  Queries value:
                                    HKLM\software\microsoft\internet
```

explorer\main\featurecontrol\feature protocol lockdown[msmpeng.exe]

HKLM\software\microsoft\windows

Queries value:

```
nt\currentversion\compatibility32[svchost]
      Queries value:
                                                                                          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[svchost]
      Oueries value:
                                                                                          HKU\.default\software\microsoft\multimedia\audio[systemformats]
      Oueries value:
                                                                                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.imaadpcm]
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
      Oueries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
      Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
      Queries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm.ima adpcm[cfilter tags]
      Queries value:
                                                                                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msadpcm]
      Oueries value:
HKLM \label{lem:hklm} \\ HKLM \label{lem:hklm} HKLM \label{lem:hklm} \\ HKLM \label{lem:hkklm} \\ HKLM \label{lem:h
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
      Queries value
HKLM \verb|\software| microsoft\audiocompression manager \verb|\driver| cache \verb|\msacm.msadpcm[aformattagcache]| and the statement of the statement 
      Oueries value:
HKLM \backslash software \backslash microsoft \backslash audio compression manager \backslash driver cache \backslash msacm. msadpcm [cfilter tags]
      Queries value:
                                                                                           HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg711]
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
      Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
                                                                                          HKLM\software\microsoft\windows
      Oueries value:
nt\currentversion\drivers32[msacm.msgsm610]
      Oueries value:
HKLM \label{lem:hklm} \\ HKLM \label{lem:hklm} HKLM \label{lem:hklm} If dws upport]
      Oueries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
      Queries value:
HKLM \verb|\software\microsoft\audiocompression| manager \verb|\driver| cache \verb|\msacm.msgsm610[aformattagcache]| aformattagcache]| the software \verb|\msacm.msgsm610[aformattagcache]| aformattagcache]| aformattagcachee]| aformattagcachee]| aformattagcachee]| aformattagcachee]| af
      Queries value
HKLM \label{lem:hklm} In the latest and in the
                                                                                          HKLM\software\microsoft\windows
      Queries value:
nt\currentversion\drivers32[msacm.trspch]
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
      Oueries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
      Oueries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
                                                                                          HKLM\software\microsoft\windows
     Oueries value:
nt\currentversion\drivers32[msacm.msg723]
      Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
      Queries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msg723[cformattags]
      Queries value:
HKLM \verb|\software\microsoft\audiocompression| manager \verb|\drivercache\misg723[aformattagcache]| \\
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
      Queries value:
                                                                                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msaudio1]
      Oueries value:
Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
      Queries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
      Oueries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msaudio1[cfiltertags]
      Oueries value:
                                                                                           HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.sl anet]
      Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[fdwsupport]
      Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[cformattags]
      Queries value:
HKLM \label{lem:hkk} In the latest and the latest
      Oueries value:
Queries value:
                                                                                           HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
       Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
      Queries value:
Queries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ mac m. iac \ 2[cfilter tags] \ driver \ cache \ mac m. iac \ 2[cfilter tags] \ driver \ cache \ mac \ mac
      Queries value:
                                                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
```

```
Oueries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. 13 acm [fdw support]
  Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
  Oueries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
  Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
                                     HKU \verb|\|.default\| software \verb|\| multimedia\| audio compression
  Oueries value:
manager\msacm[nopcmconverter]
  Queries value:
                                     HKU\.default\software\microsoft\multimedia\audio compression
manager\priority v4.00[priority1]
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
  Queries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
  Queries value:
                                     HKLM\system\currentcontrolset\control\productoptions[producttype]
                                     HKU\.default\software\microsoft\windows\currentversion\explorer\user
  Oueries value:
shell folders[personal]
  Queries value:
                                     HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local settings]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
  Queries value:
HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| the memanager [compositing]| |
  Queries value:
                                     HKU\.default\control panel\desktop[lamebuttontext]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer[nofilefolderconnection]
  Oueries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature protocol lockdown[svchost.exe]
                                     HKCR\directory\shellex\copyhookhandlers\cdf[]
  Queries value:
                                     HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32[]
  Oueries value:
  Oueries value:
                                     HKCR\clsid\{67ea19a0-ccef-11d0-8024-
00c04fd75d13}\inprocserver32[loadwithoutcom]
                                    HKLM\software\microsoft\windows\currentversion\shell
  Queries value:
extensions\blocked[{67ea19a0-ccef-11d0-8024-00c04fd75d13}]
                                     \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \shell \end{tabular}
  Oueries value:
extensions\blocked[{67ea19a0-ccef-11d0-8024-00c04fd75d13}]
                                     HKLM\software\microsoft\windows\currentversion\shell
Queries value:
                                     \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{microsoft} \windows \current version} \end{tabular} \label{thm:local_hammon_hammon}
extensions\cached[{67ea19a0-ccef-11d0-8024-00c04fd75d13} {00000000-0000-0000-c000-0000000000046}
0x4011
  Queries value:
                                     HKCR\clsid\{67ea19a0-ccef-11d0-8024-
00c04fd75d13}\inprocserver32[inprocserver32]
                                     HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}[appid]
  Queries value:
  Oueries value:
                                     HKCR\clsid\{67ea19a0-ccef-11d0-8024-
00c04fd75d13}\inprocserver32[threadingmodel]
                                     HKCR\directory\shellex\copyhookhandlers\filesystem[]
  Oueries value:
  Oueries value:
                                     HKCR\clsid\{217fc9c0-3aea-1069-a2db-08002b30309d}\inprocserver32[]
                                     HKCR\directory\shellex\copyhookhandlers\mydocuments[]
  Oueries value:
                                     HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32[]
  Oueries value:
                                     HKCR\clsid\{ecf03a33-103d-11d2-854d-
  Oueries value:
006008059367}\inprocserver32[loadwithoutcom]
                                     HKLM\software\microsoft\windows\currentversion\shell
  Queries value:
extensions\blocked[{ecf03a33-103d-11d2-854d-006008059367}]
                                     HKCU\software\microsoft\windows\currentversion\shell
  Queries value:
extensions\blocked[{ecf03a33-103d-11d2-854d-006008059367}]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\shell
extensions \\ \\ cached [ \{ecf03a33-103d-11d2-854d-006008059367\} \\ \{00000000-0000-0000-c000-00000000000046\} \\ \\ \\ \\ extensions \\ \\ \\ \\ extensions \\ \\ extension
0x4011
                                     HKCU\software\microsoft\windows\currentversion\shell
  Queries value:
extensions\cached[{ecf03a33-103d-11d2-854d-006008059367} {00000000-0000-0000-c000-000000000046}}
0x401]
  Queries value:
                                     HKCR\clsid\{ecf03a33-103d-11d2-854d-
006008059367}\inprocserver32[inprocserver32]
  Queries value:
                                     \label{localized} $HKCR\clsid{ecf03a33-103d-11d2-854d-006008059367} [appid] $$
  Queries value:
                                     HKCR\clsid\{ecf03a33-103d-11d2-854d-
006008059367}\inprocserver32[threadingmodel]
                                     HKCR\directory\shellex\copyhookhandlers\sharing[]
  Oueries value:
                                     HKCR \verb|\clsid| \{40dd6e20-7c17-11ce-a804-00aa003ca9f6\} \verb|\inprocserver32[]|
  Oueries value:
                                     HKCR\clsid\{40dd6e20-7c17-11ce-a804-
  Oueries value:
00aa003ca9f6}\inprocserver32[loadwithoutcom]
                                     HKLM\software\microsoft\windows\currentversion\shell
  Oueries value:
extensions\blocked[{40dd6e20-7c17-11ce-a804-00aa003ca9f6}]
                                     HKCU\software\microsoft\windows\currentversion\shell
  Queries value:
extensions\blocked[{40dd6e20-7c17-11ce-a804-00aa003ca9f6}]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{40dd6e20-7c17-11ce-a804-00aa003ca9f6} {00000000-0000-0000-c000-0000000000046}}
0x401]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{40dd6e20-7c17-11ce-a804-00aa003ca9f6} {00000000-0000-0000-c000-00000000046}}
0x401]
  Queries value:
                                     HKCR\clsid\{40dd6e20-7c17-11ce-a804-
00aa003ca9f6}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}[appid]
                                     HKCR\clsid\{40dd6e20-7c17-11ce-a804-
  Queries value:
00aa003ca9f6}\inprocserver32[threadingmodel]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+explorer\+user\ shell
folders[local settings]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileimagepath]
```

```
Oueries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[fonts]
   Oueries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[startup]
   Oueries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[programs]
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[start menu]
  Oueries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[recent]
  Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[sendto]
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[favorites]
   Queries value:
                                                 \label{local-observation} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}}
folders[nethood]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[printhood]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[templates]
                                                 HKLM\software\microsoft\windows\currentversion\explorer\user shell
   Queries value:
folders[common startup]
   Queries value:
                                                 HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common programs]
   Queries value:
                                                 \label{lem:hklmsoftware} \begin{tabular}{l} HKLM \end{tabular} soft \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} user shell
folders[common start menu]
   Queries value:
                                                 \label{lem:hklmsoftware} \begin{tabular}{l} HKLM \end{tabular} soft \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} user shell
folders[common favorites]
   Queries value:
                                                 HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
   Queries value:
                                                 HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common templates]
   Oueries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[altstartup]
   Queries value:
                                                 HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common altstartup]
   Oueries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my pictures]
   Queries value:
                                                 HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
   Queries value:
                                                 HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)]
   Queries value:
                                                 HKLM\software\microsoft\windows\currentversion[commonfilesdir]
                                                 \label{local-observation} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}}
   Queries value:
folders[administrative tools]
   Queries value:
                                                 \label{lem:hklmsoftware} \begin{tabular}{l} HKLM \end{tabular} soft \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} user shell
folders[common administrative tools]
   Queries value:
                                                 HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
   Queries value:
                                                 HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
   Oueries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my music]
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[mv video]
                                                 HKLM\software\microsoft\windows\currentversion\explorer\user shell
   Queries value:
folders[commonpictures]
  Queries value:
                                                 HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[commonmusic]
   Queries value:
                                                 HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[commonvideo]
   Queries value:
                                                 \label{lem:hklmsoftware} \begin{tabular}{l} HKLM \end{tabular} soft \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} user shell
folders[oem links]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cd burning]
   Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[2106]
  Oueries value:
                                                 HKLM\software\microsoft\windows\currentversion\internet
settings\zones\0[2106]
  Queries value:
                                                 HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1400]
                                                 HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonintranet]
  Queries value:
                                                 HKLM\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
                                                 HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zonemap[autodetect]
                                                 HKCR\clsid\{50d5107a-d278-4871-8989-
  Queries value:
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                                                 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-
   Queries value:
f4ceaaf59cfc}\inprocserver32[threadingmodel]
                                                 - \\ HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 80d8
   Oueries value:
c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable]
                                                 HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32[inprocserver32]
                                                 HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]
   Queries value:
                                                 HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid]
   Queries value:
   Queries value:
                                                 HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32[threadingmodel]
   Queries value:
                                                 HKCR\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32[inprocserver32]
                                                 \label{local-eq:hkcr} $$ HKCR\clsid_{a4b544a1-438d-4b41-9325-869523e2d6c7} \in \clsid_{a4b544a1-438d-4b41-9325-869523e2d6c7} $$ inprocessor (a) $$ (a) $$ (a) $$ (a) $$ (b) $$ (b) $$ (b) $$ (b) $$ (b) $$ (c) $$ (c
   Queries value:
```

```
Oueries value:
                                                HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]
   Oueries value:
                                               HKCR\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32[threadingmodel]
   Oueries value:
                                               HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description]
                                               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
   Oueries value:
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description]
   Oueries value:
                                               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[description]
   Oueries value:
                                               \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet settings \verb+ vurled to the software \verb+ windows \verb+ current version \verb+ internet settings \verb+ vurled to the software \verb+ windows windows \verb+ windows \verb+ windows w
history[daystokeep]
   Queries value:
                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[inprocserver32]
   Queries value:
                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[]
                                                HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[appid]
   Queries value:
   Queries value:
                                                HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
   Oueries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1201]
   Queries value:
                                                HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Queries value:
                                               HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:
                                                HKLM\software\microsoft\ole[defaultaccesspermission]
   Oueries value:
                                                HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
   Oueries value:
                                               HKCU\software\microsoft\windows\currentversion\internet
settings[cointernetcombineiuricachesize]
   Oueries value:
                                               \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[cointernetcombineiuricachesize]
                                               HKCR\clsid\{81397204-f51a-4571-8d7b-
   Oueries value:
dc030521aabd}\inprocserver32[inprocserver32]
                                               HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[]
   Oueries value:
                                               HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[appid]
   Queries value:
                                               HKCR\clsid\{81397204-f51a-4571-8d7b-
   Queries value:
dc030521aabd}\inprocserver32[threadingmodel1
                                               HKCR\clsid\{d1fe6762-fc48-11d0-883a-
   Oueries value:
3c8b00c10000}\inprocserver32[inprocserver32]
                                               HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[]
   Queries value:
                                               HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}[appid]
   Oueries value:
                                               HKCR\clsid\{d1fe6762-fc48-11d0-883a-
   Oueries value
3c8b00c10000}\inprocserver32[threadingmodel]
   Queries value:
                                               HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_behaviors[flashplayer18\_a\_install.exe]|
                                               HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature behaviors[*]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\zones\0[2000]
   Queries value:
                                                HKLM\software\microsoft\internet explorer\default
behaviors[dxtfilterbehavior]
   Queries value:
                                               HKCR\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[inprocserver32]
   Oueries value:
                                               HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[]
                                               HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}[appid]
   Oueries value:
   Oueries value:
                                               HKCR\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[threadingmodel]
                                               HKLM\hardware\devicemap\video[maxobjectnumber]
   Oueries value:
                                                HKLM\hardware\devicemap\video[\device\video0]
   Oueries value:
   Queries value:
                                                HKLM\hardware\devicemap\video[\device\video1]
   Queries value:
                                                HKLM\hardware\devicemap\video[\device\video2]
                                                HKLM\software\microsoft\directdraw\compatibility\bug![name]
   Queries value:
   Queries value:
                                                HKLM\software\microsoft\directdraw\compatibility\bug![flags]
   Queries value:
                                                HKLM\software\microsoft\directdraw\compatibility\bug![id]
   Queries value:
                                                HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus demolition derby 2 [name]
   Queries value:
                                                HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus demolition derby 2 [flags]
                                                HKLM\software\microsoft\directdraw\compatibility\demolitionderby2[id]
   Queries value:
   Queries value:
                                                HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[name]
   Queries value:
                                                \label{thm:local_ham} \begin{tabular}{ll} HKLM \software \verb|\mbox{microsoft} \directdraw \compatibility \verb|\mbox{mortalkombat3[flags]} \end{tabular}
   Queries value:
                                                HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus mortal kombat \\ 3[id]
   Oueries value:
                                                HKLM\software\microsoft\directdraw\compatibility\msgolf98[name]
   Oueries value:
                                                HKLM\software\microsoft\directdraw\compatibility\msgolf98[flags]
   Oueries value:
                                                HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus msgolf 98[id]
   Oueries value:
                                                HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus nhlpowerplay [name]
   Oueries value:
                                                HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus nhlpowerplay [flags]
                                                HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[id]
   Oueries value:
                                                HKLM \verb|\software\microsoft\directdraw\compatibility\nortonsysteminfo[name]
   Oueries value:
                                                HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\nortons y steminfo[flags]|
   Oueries value:
   Oueries value:
                                                HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus norton system in fo[id]
   Oueries value:
                                                HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name]
                                                HKLM\software\microsoft\directdraw\compatibility\rogue squadron[flags]
   Queries value:
                                                HKLM\software\microsoft\directdraw\compatibility\rogue squadron[id]
   Queries value:
                                                HKLM\software\microsoft\directdraw\compatibility\savage[name]
   Queries value:
   Queries value:
                                                HKLM\software\microsoft\directdraw\compatibility\savage[flags]
   Queries value:
                                                HKLM\software\microsoft\directdraw\compatibility\savage[id]
   Queries value:
                                                HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[name]
   Oueries value:
                                                HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[flags]
   Oueries value:
                                                HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[id]
                                                HKLM\software\microsoft\directdraw\compatibility\silentthunder[name]
   Queries value:
   Queries value:
                                                HKLM\software\microsoft\directdraw\compatibility\silentthunder[flags]
   Queries value:
                                                HKLM\software\microsoft\directdraw\compatibility\silentthunder[id]
   Oueries value:
                                                HKLM\software\microsoft\directdraw\compatibility\terracide[name]
   Queries value:
                                                HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus terracide [flags]
   Queries value:
                                                HKLM\software\microsoft\directdraw\compatibility\terracide[id]
   Queries value:
                                                HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus third dimension [name]
   Queries value:
                                                HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus third dimension [flags]
   Oueries value:
                                                HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus third dimension [id]
```

Queries value:

```
HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus ziff davis quality benchmark [name]
  Oueries value
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[flags]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdayisqualitybenchmark[id]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
  Queries value:
                                       HKLM\software\microsoft\directdraw[modexonly]
  Queries value:
                                       HKLM\software\microsoft\directdraw[emulationonly]
  Queries value:
                                        HKLM\software\microsoft\directdraw[showframerate]
  Queries value:
                                       HKLM\software\microsoft\directdraw[enableprintscreen]
  Queries value:
                                        HKLM\software\microsoft\directdraw[forceagpsupport]
  Oueries value:
                                        HKLM\software\microsoft\directdraw[disableagpsupport]
                                        HKLM\software\microsoft\directdraw[disablemmx]
  Oueries value:
                                        HKLM\software\microsoft\directdraw[disableddscapsinddsd]
   Queries value:
  Queries value:
                                        HKLM\software\microsoft\directdraw[disablewidersurfaces]
  Queries value:
                                        HKLM\software\microsoft\directdraw[usenonlocalvidmem]
  Oueries value:
                                       HKLM\software\microsoft\directdraw[forcerefreshrate]
  Oueries value:
                                       HKLM\software\microsoft\direct3d[flipnovsync]
  Oueries value:
                                       HKLM\software\microsoft\directdraw[owndc]
  Queries value:
                                       HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[inprocserver32]
                                       \label{lem:hkcr} $$ HKCR\clsid_{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe} \sin 2\theta e^{-\theta} e^
  Queries value:
                                       HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[appid]
  Queries value:
                                       HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
  Oueries value:
f941e9b7e1fe}\inprocserver32[threadingmodel]
                                       HKCR\dximagetransform.microsoft.gradient\clsid[]
  Queries value:
                                       HKCR\clsid\{623e2882-fc0e-11d1-9a77-
  Queries value:
0000f8756a10}\inprocserver32[inprocserver32]
                                       HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32[]
  Oueries value:
                                       HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}[appid]
  Oueries value:
                                       HKCR\clsid\{623e2882-fc0e-11d1-9a77-
  Queries value:
0000f8756a10}\inprocserver32[threadingmodel]
  Oueries value:
                                       HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpdomain]
                                       HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:
c7d49d7cecdc}[enabledhcp]
  Queries value:
c7d49d7cecdc}[leaseobtainedtime]
  Queries value:
c7d49d7cecdc}[leaseterminatestime]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
                                       HKLM\software\microsoft\rpc\securityservice[10]
  Oueries value:
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
  Queries value:
c7d49d7cecdc}[dhcpnameserver]
  Queries value:
                                       \label{lem:hklm} \verb+Kklm \system \current control set \services \netbt \parameters [nodetype]
   Queries value:
                                        HKLM\system\currentcontrolset\services\netbt\parameters[dhcpnodetype]
   Queries value:
                                        HKLM\system\currentcontrolset\services\netbt\parameters[scopeid]
  Queries value:
                                       HKLM\system\currentcontrolset\services\netbt\parameters[dhcpscopeid]
                                       HKLM\system\currentcontrolset\services\tcpip\parameters[ipenablerouter]
   Queries value:
  Queries value:
                                       HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
  Oueries value:
HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus msaps spc.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\services\netbt\parameters[enableproxy]
  Oueries value:
  Oueries value:
                                       HKLM\system\currentcontrolset\services\netbt\parameters[enabledns]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
  Queries value:
                                       HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:
                                       HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
                                       HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
  Queries value:
                                       HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
                                       HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
  Queries value:
                                       HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
   Queries value:
  Queries value:
                                       HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
Queries value:
Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
  Oueries value:
HKLM \verb|\system| current control \verb|\spicache| msnsspc.dll[name]|
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
  Oueries value:
  Oueries value:
HKLM\svstem\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
                                   Oueries value:
  Oueries value:
                                    HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
  Queries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
  Queries value:
                                    HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
  Queries value:
                                   HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows nt\currentversion\winlogon[parseautoexec]
                                   HKCR\clsid\{c6365470-f667-11d1-9067-
  Oueries value
00c04fd9189d}\inprocserver32[inprocserver32]
  Queries value:
                                   HKU\s-1-5-21-1757981266-507921405-1957994488-1003\control
panel\desktop[multiuilanguageid]
  Oueries value:
                                    HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserver32[]
  Queries value:
                                   HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}[appid]
  Oueries value:
                                   HKCR\clsid\{c6365470-f667-11d1-9067-
00c04fd9189d}\inprocserver32[threadingmodel]
  Oueries value:
                                   \label{lem:hkul.default} HKU\.default\software\microsoft\windows\current\version\sline\color{lem:hkul.default\software\microsoft\windows\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\cur
settings[fromcachetimeout]
  Queries value:
                                   HKU\.default\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
                                   \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
  Oueries value:
settings[secureprotocols]
                                   HKCR\clsid\{4cb26c03-ff93-11d0-817e-
  Queries value:
0000f87557db}\inprocserver32[inprocserver32]
                                   HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[certificaterevocation]
                                   HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[certificaterevocation]
  Oueries value:
                                   HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings[disablekeepalive]
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[disablepassport]
  Queries value:
                                   HKU\.default\software\microsoft\windows\currentversion\internet
settings[idnenabled]
                                    Queries value:
  Queries value:
                                    HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings[cachemode]
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Oueries value:
                                   HKU\.default\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                                    HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[appid]
  Oueries value:
  Oueries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[proxvhttp1.1]
                                   HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[enablenegotiate]
                                   \label{lem:hkuldefault} $$HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablebasicoverclearchannel]
                                    HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[clientauthbuiltinui]
  Queries value:
                                   HKU\.default\software\microsoft\windows\currentversion\internet
settings[syncmode5]
                                   HKCR\clsid\{4cb26c03-ff93-11d0-817e-
  Queries value:
0000f87557db}\inprocserver32[threadingmodel]
  Queries value:
                                   HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings\5.0\cache[signature]
  Oueries value:
                                   HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings\5.0\cache\content[peruseritem]
  Oueries value:
                                   HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\explorer\user shell folders[cache]
                                   HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[cacheprefix]
  Queries value:
                                   HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
                                   HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\cookies[peruseritem]
                                   HKU\s-1-5-21-1757981266-507921405-1957994488-
  Queries value:
1003\software\microsoft\windows\currentversion\explorer\user shell folders[cookies]
                                   HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\cookies[cacheprefix]
                                   HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\cookies[cachelimit]
  Oueries value:
                                   HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings\5.0\cache\history[peruseritem]
  Queries value:
                                   HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[inprocserver32]
                                   HKU\s-1-5-21-1757981266-507921405-1957994488-
  Queries value:
1003\software\microsoft\windows\currentversion\explorer\user shell folders[history]
  Queries value:
                                   HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\nprocserver32[]
  Queries value:
                                   HKCR \clsid \ \{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd\} [appid]
  Queries value:
                                   HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\explorer\shell folders[cache]
  Queries value:
                                   HKU\.default\software\microsoft\windows\currentversion\internet
```

```
settings\5.0\cache\history[cacheprefix]
                                     HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\history[cachelimit]
  Oueries value:
                                     HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Oueries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                                    HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                                    HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
                                    HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                                    HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
  Queries value:
f4fc1e6ca1bd}\inprocserver32[threadingmodel]
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012013122320131224[cacherepair]
  Oueries value
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012013122320131224[cachepath]
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012013122320131224[cacheprefix]
                                    HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012013122320131224[cachelimit]
  Queries value:
                                    \label{lem:hkuldefault} $$HKU\.default\software\microsoft\windows\currentversion\internet$$
settings\5.0\cache\extensible cache\mshist012013122320131224[cacheoptions]
  Queries value
                                    \label{lem:hkul.default} HKU\.default\software\microsoft\windows\current\version\sline\color{lem:hkul.default\software\microsoft\windows\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\current\cur
{\tt settings[disableworkerthreadhibernation]}
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                                    HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[socketsendbufferlength]
                                    HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\compatibilitv32[dllhost]
  Oueries value:
                                    HKLM\software\microsoft\windows nt\currentversion\ime
compatibilitv[dllhost]
                                     HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]
  Queries value:
  Oueries value:
                                    HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings[socketreceivebufferlength]
  Oueries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
  Queries value:
                                     HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings[maxhttpredirects]
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                                    \label{lem:hkuldefault} $$HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxconnectionsper1_0server]
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
  Oueries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Oueries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                                    HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[connectretries]
                                    HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[sendtimeout]
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                                     HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[]
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablentlmpreauth]
  Queries value:
                                    \label{lem:hkul.default} HKU\.default\software\microsoft\windows\currentversion\sline internet
settings[scavengecachelowerbound]
  Queries value:
                                     HKU\.default\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                                    HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
  Oueries value
settings\5.0\cache[scavengecachefilelimit]
  Queries value:
                                    HKCR \ typelib \ \{54314d1d-35fe-11d1-81a1-0000f87557db\} \ 1.1 \ 0 \ win 32[]
  Oueries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback[svchost.exe]
                                    HKCU \backslash software \backslash microsoft \backslash multimedia \backslash audio [system for mats] \\
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablecachingofsslpages]
                                    HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablecachingofsslpages]
                                    HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[perusercookies]
  Oueries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
  Queries value:
                                    HKU\.default\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
  Queries value:
                                    HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings[dialupuselansettings]
  Queries value:
                                     HKCU\software\microsoft\ftp[use web based ftp]
  Queries value:
                                     HKCU\software\microsoft\internet
explorer\services[selectionactivitybuttondisable]
  Oueries value:
                                    \label{lem:hkul.default} HKU\.default\software\microsoft\windows\currentversion\sline internet
settings[sendextracrlf]
```

```
HKU\.default\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[bypassftptimecheck]
   Oueries value:
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
   Oueries value:
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[wpadsearchalldomains]
   Queries value:
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
settings[disable]egacypreauthasserver]
                                                       HKCU\software\microsoft\internet explorer\suggested sites[enabled]
    Queries value:
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
   Queries value:
settings[bypasshttpnocachecheck]
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
    Queries value:
settings[bypasssslnocachecheck]
                                                       \label{lem:hkuldefault} $$HKU\.default\software\microsoft\windows\currentversion\internet
    Queries value:
settings[nocheckautodialoverride]
    Oueries value:
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
    Queries value:
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
    Oueries value:
                                                       HKCR\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprocserver32[inprocserver32]
    Oueries value:
                                                       \label{lem:hkuldefault} $$HKU\.default\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
   Queries value:
                                                       \label{lem:hkul.default} HKU\.default\software\microsoft\windows\currentversion\sline internet
settings[dnscacheenabled]
   Queries value:
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[dnscachetimeout]
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
   Queries value:
settings[warnonpost]
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[warnalwaysonpost]
                                                       \label{thm:local_HKU} \begin{tabular}{ll} HKU\label{thm:local_HKU} Algorithms $$ \current version \end{tabular} $$ in terms $$ \current version \end{tabular} $$ in the substitution $$ \current version \end{tabular} $$ in
   Queries value:
settings[warnonzonecrossing]
   Queries value:
                                                       HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings[warnonbadcertsending]
    Queries value:
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
    Queries value:
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
settings[warno
                                npostredirect]
                                                        \label{locality} HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[]
    Queries value:
                                                       \label{lem:hkuldefault} $$HKU\.default\software\microsoft\windows\currentversion\internet
    Queries value:
settings[alwaysdrainonredirect]
   Queries value:
                                                       \label{lem:hkul.default} HKU\.default\software\microsoft\windows\currentversion\sline internet
settings[warnonhttpstohttpredirect]
   Oueries value:
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
   Oueries value
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
settings[enableautodial]
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[truncatefilename]
                                                       HKU\.default\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[badproxyexpirestime]
                                                       HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}[appid]
    Queries value:
   Queries value:
                                                       HKCU\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
    Queries value:
                                                       HKCR\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprocserver32[threadingmodel]
    Queries value:
                                                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[svchost.exe]
                                                        HKCU\software\microsoft\multimedia\audio compression manager\priority
    Queries value
v4.00[priority1]
    Queries value
HKLM \label{lem:hklm} In the lambda \label{lem:hklm} HKLM \label{lem:hklm} In the lambda \label{lem:hkklm} In the lambda \label{l
    Queries value:
                                                        HKLM\software\microsoft\tracing[enableconsoletracing]
    Oueries value:
                                                        HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
    Oueries value:
                                                        HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
    Queries value:
                                                        HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
    Queries value:
                                                        HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32 [consoletracing mask] \\
                                                        HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32 [maxfilesize]
    Oueries value:
                                                       HKLM\software\microsoft\tracing\rasapi32[filedirectory]
    Oueries value:
                                                        HKU\s-1-5-21-1757981266-507921405-1957994488-
    Queries value:
1003\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
                                                       HKU\s-1-5-21-1757981266-507921405-1957994488-
    Queries value:
1003\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
                                                       HKU\s-1-5-21-1757981266-507921405-1957994488-
   Queries value:
1003\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]
    Oueries value:
                                                       HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
                                                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[dllhost.exe]
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} which is a property of the local prop
    Queries value
Oueries value
{\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ tcpip \verb|\ parameters [usedomain name devolution]| \\
```

```
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
  Oueries value
HKLM\system\currentcontrolset\services\dnscache\parameters[allowungualifiedguery]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowungualifiedguery]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
  Queries value:
                                  HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
  Queries value:
\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ tcpip \+ parameters \[disable dynamic update]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
  Queries value:
HKLM \label{lem:hkk} In the latest and the latest
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration ttl]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]
  Queries value:
Oueries value
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
  Oueries value
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
  Oueries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
  Queries value:
Queries value:
                                   HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [dns test]
  Queries value:
                                   HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [max cache size]
  Queries value:
                                   HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [server priority time limit]
  Oueries value
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
  Queries value
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters[dnsmulticast query timeouts]| \\
  Queries value:
c7d49d7cecdc}[queryadaptername]
  Queries value:
c7d49d7cecdc}[disableadapterdomainname]
  Oueries value:
c7d49d7cecdc}[registrationenabled]
  Queries value:
c7d49d7cecdc}[registeradaptername]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationmaxaddresscount]
  Oueries value:
c7d49d7cecdc}[maxnumberofaddressestoregister]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[domain]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[ipautoconfigurationenabled]
  Queries value:
c7d49d7cecdc}[addresstype]
                                      HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
   Queries value:
HKLM \verb|\system| current controls et \verb|\services| tcpip \verb|\parameters[dnsnbtlookuporder]|
  Queries value:
                                     \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ cryptography\+ defaults\+ provider\+ microsoft\+ strong
cryptographic provider[type]
  Queries value:
                                     HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value:
                                     HKLM\software\microsoft\internet
\verb|explorer| main\featurecontrol\feature_subdownload_lockdown[flashplayer18\_a_install.exe]|
  Queries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[*]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
                                     HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\user agent[compatible]
  Oueries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\user agent[version]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
                                     \label{thm:linear} \mbox{HKCU\software\mbox{\sc urrentversion\internet settings[user thm])} is the linear constant of the linear consta
  Queries value:
agent]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
  Oueries value:
                                     \label{lem:hklm} \verb+Kklm\+ software\+ incressft\+ windows\+ current version\+ internet
settings\5.0\user agent[platform]
  Oueries value:
                                     HKCU\software\microsoft\windows script\settings[jitdebug]
  Oueries value:
                                     HKCR\http\shell\open\command[]
  Oueries value:
                                     HKLM\software\microsoft\internet explorer\main[maxrenderline]
                                     HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\connections[winhttpsettings]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\connections[defaultconnectionsettings]
  Queries value:
                                     HKLM\software\microsoft\cryptography[machineguid]
  Queries value:
                                     HKCR\.png[content type]
  Queries value:
                                     HKCR\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
                                      HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[appid]
   Queries value:
                                     HKCR\clsid\{30c3b080-30fb-11d0-b724-
  Queries value
00aa006c1a01}\inprocserver32[threadingmodel]
  Queries value:
                                     HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[inprocserver32]
  Oueries value:
                                     \label{locality} $$ HKCR\clsid_{6a01fda0-30df-11d0-b724-00aa006c1a01}\times [] $$
  Oueries value:
                                     HKCR \verb|\clsid|{6a01fda0-30df-11d0-b724-00aa006c1a01}{[appid]}
  Oueries value:
                                     HKCR\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32[threadingmodel]
                                     HKCR\mbox{\tt Mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt type} \mbox{\tt bits} \mbox{\tt [0]}
  Oueries value:
  Queries value:
                                      HKCR\mime\database\content type\image/gif\bits[0]
  Oueries value:
                                      HKCR\mbox{\tt mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt image/jpeg} \mbox{\tt bits} \mbox{\tt [0]}
  Oueries value:
                                      HKCR\mime\database\content type\image/pjpeg\bits[0]
  Oueries value:
                                      HKCR\mime\database\content type\image/png\bits[0]
                                      HKCR\mime\database\content type\image/x-png\bits[0]
  Queries value:
  Queries value:
                                      HKCR\mime\database\content type\image/x-wmf\bits[0]
                                      HKCR\mime\database\content type\image/x-png[image filter clsid]
  Queries value:
  Queries value:
                                     HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[inprocserver32]
                                     HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
  Queries value:
  Oueries value:
                                     HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid]
  Oueries value:
                                     HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32[threadingmodel]
  Sets/Creates value:
                                      HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[displayname]
  Sets/Creates value:
                                      HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus new product
1.00[displayversion]
  Sets/Creates value:
                                      HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus new product
1.00[versionmajor]
  Sets/Creates value:
                                      HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus new product
```

HKLM\software\microsoft\windows\currentversion\uninstall\newproduct

1.00[versionminor]
Sets/Creates value:

```
1.00[publisher]
   Sets/Creates value:
                                        HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[displayicon]
  Sets/Creates value:
                                        HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[uninstallstring]
                                        HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
   Sets/Creates value:
1.00[urlinfoabout]
  Sets/Creates value:
                                        HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[helplink]
  Sets/Creates value:
                                        HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[installlocation]
  Sets/Creates value:
                                        HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[installsource]
   Sets/Creates value:
                                        HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[installdate]
   Sets/Creates value:
                                        HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus new product
1.00[language]
   Sets/Creates value:
                                        HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[estimatedsize]
   Sets/Creates value:
                                        HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus new product
1.00[nomodify]
  Sets/Creates value:
                                        HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus new product
1.00[norepair]
  Sets/Creates value:
                                        HKCU\software\microsoft\windows\shellnoroam\muicache[c:\program
files\flashplayer18_a_install.exe]
   Sets/Creates value:
                                        HKCU\software\microsoft\windows\shellnoroam\muicache[c:\program
files\install.exel
   Sets/Creates value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\docume~1\admin\locals~1\temp\rarsfx0\msmpeng.exe]
                                        HKLM\system\currentcontrolset\services\devicesync[description]
  Sets/Creates value:
                                        HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:
   Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}[baseclass]
                                        HKCU\software\microsoft\windows\currentversion\explorer\shell
   Value changes:
folders[personal]
   Value changes:
                                        HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common documents]
   Value changes:
                                        HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
   Value changes:
                                        \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \software \verb|\microsoft| windows \current version \explorer \shell \end{tabular}
folders[common desktop]
   Value changes:
                                        HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
                                        \label{thm:local_thm:local_thm} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc 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\+ internet
settings\zonemap[autodetect]
  Value changes:
                                        HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
                                        HKCU\software\microsoft\windows\currentversion\explorer\shell
  Value changes:
folders[cookies]
                                        HKCU\software\microsoft\windows\currentversion\explorer\shell
  Value changes:
folders[local appdata]
  Value changes:
                                        HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[history]
                                        HKLM\system\currentcontrolset\services\devicesync[type]
  Value changes:
   Value changes:
                                        HKLM\software\microsoft\directdraw\mostrecentapplication[name]
   Value changes:
                                        HKLM\software\microsoft\directdraw\mostrecentapplication[id]
   Value changes:
                                        HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\explorer\shell folders[cache]
                                        HKU\s-1-5-21-1757981266-507921405-1957994488-
   Value changes:
1003\software\microsoft\windows\currentversion\explorer\shell folders[cookies]
   Value changes:
                                        HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\explorer\shell folders[history]
  Value changes:
                                        HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common appdata]
  Value changes:
                                        HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\explorer\shell folders[appdata]
                                        HKU\s-1-5-21-1757981266-507921405-1957994488-
  Value changes:
1003\software\microsoft\windows\currentversion\internet settings[proxyenable]
   Value changes:
                                        HKU\s-1-5-21-1757981266-507921405-1957994488-
1003 \land software \verb|\microsoft| windows \verb|\currentversion| internet settings \verb|\connections[savedlegacysettings]| in the property of the prope
```