Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details Host: mag2, Sample ID: 469, Task ID: 475

Task ID: 475

Risk Level: 10

Date Processed: 2016-03-24 13:55:15 (UTC)

Processing Time: 61.79 seconds Virtual Environment: IntelliVM

Execution Arguments:

"c:\windows\temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe"

Sample ID: 469 basic Type: Owner: admin

Label: 755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63

Date Added: 2016-03-24 13:55:14 (UTC)

PE32:win32:gui File Type: 1580101 bytes File Size:

cba74e507e9741740d251b1fb34a1874 MD5:

SHA256: 755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63

Description:

Pattern Matching Results

3 Writes to a log file [Info]

SSL traffic on standard port

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

3 Connects to local host

5 Possible process injection

5 Installs service

5 Opens Copy Hook Handlers key 3 Long sleep detected

Starts process from Application Data folder

1 YARA score 1

2 Terminates third-party processes

3 HTTP connection - response code 200 (success)

Static Events

YARA rule hit: Nonexecutable PE: Contains a virtual section Anomaly:

Process/Thread Events

C:\WINDOWS\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe $["c:\windows\temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe"]$ C:\Program Files\flashplayer18_a_install.exe ["C:\Program Creates process:

Files\flashplayer18_a_install.exe"]

C:\Program Files\install.exe ["C:\Program Files\install.exe"] Creates process:

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] Creates process:

C:\WINDOWS\system32\dllhost.exe [C:\WINDOWS\System32\dllhost.exe -user] Creates process:

PID:1112 C:\WINDOWS\system32\svchost.exe Writes to process: PID:1032 C:\WINDOWS\system32\svchost.exe Writes to process: PID:1092 C:\WINDOWS\system32\dllhost.exe Writes to process:

Terminates process:

C:\WINDOWS\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe

Terminates process: C:\Documents and Settings\All Users\Application

Data\Microsoft\DeviceSync\MsMpEng.exe

Terminates process: C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFX0\MsMpEng.exe

Terminates process: C:\Program Files\install.exe

Named Object Events

,	
Creates mutex:	\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003	
Creates mutex:	\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003	
Creates mutex:	\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003	
Creates mutex:	\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003	
Creates mutex:	\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003	
Creates mutex:	\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-
507921405-1957994488	3-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\ZonesCounterMutex
Creates mutex:	\BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex:	\BaseNamedObjects\ZonesCacheCounterMutex

Creates mutex: \BaseNamedObjects\ZonesLockedCacheCounterMutex Creates mutex: **\BaseNamedObjects\oleacc-msaa-loaded** Creates mutex: \BaseNamedObjects\Adobe_ADM.log

\BaseNamedObjects\c:!documents and settings!admin!local Creates mutex: settings!temporary internet files!content.ie5! Creates mutex: $\verb|\BaseNamedObjects\c:!documents| and settings! admin! cookies!$ Creates mutex: $\verb|\BaseNamedObjects| c: ! documents and settings! admin! local|$ settings!history!history.ie5! \BaseNamedObjects\WininetConnectionMutex Creates mutex: Creates mutex: \BaseNamedObjects\!PrivacIE!SharedMemorv!Mutex \BaseNamedObjects_SHuassist.mtx Creates mutex: \BaseNamedObjects\BB6cmqyHzy8kkcJ Creates mutex: \BaseNamedObjects\SHIMLIB LOG MUTEX Creates mutex: Creates mutex: \BaseNamedObjects\DDrawWindowListMutex Creates mutex: \BaseNamedObjects\DDrawDriverObjectListMutex Creates mutex: \BaseNamedObjects__DDrawExclMode \BaseNamedObjects__DDrawCheckExclMode_ Creates mutex: \BaseNamedObjects\Adobe_GDE.log Creates mutex: Creates mutex: \BaseNamedObjects\MSIMGSIZECacheMutex \BaseNamedObjects\DINPUTWINMM Creates event: \BaseNamedObjects\userenv: User Profile setup event Creates event: \BaseNamedObjects\ShellCopyEngineRunning Creates event: Creates event: \BaseNamedObjects\ShellCopyEngineFinished Creates event: \BaseNamedObjects\CancelPort{A91D59EC-724C-4209-9B91-75BDF5A5A275} Creates event: \BaseNamedObjects\CancelPort{581E55A3-F365-4B2A-86CF-B362AF84DBE8} 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} \BaseNamedObjects\{A925355A-7A05-4070-B3BC-3D323F229F91}} Creates semaphore: File System Events Creates: C:\Documents and Settings\Admin\Local Settings\Temp\\$inst C:\Documents and Settings\Admin\Local Settings\Temp\\$inst\2.tmp Creates: C:\Documents and Settings\Admin\Local Settings\Temp\\$inst\temp_0.tmp Creates: C:\Program Files\install.exe Creates: Creates: C:\Program Files\flashplayer18_a_install.exe Creates: C:\Program Files\Adobe\NewProduct Creates: C:\Program Files\Adobe\NewProduct\Uninstall.exe Creates: C:\Program Files\Adobe\NewProduct\Uninstall.ini Creates: C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\E431E95C-97F5-44D2-A2D6-07B00F1A955B C:\Documents and Settings\Admin\Local Settings\Temp\Adobe_ADMLogs Creates: Creates: C:\Documents and Settings\Admin\Local Settings\Temp\Adobe_ADMLogs\Adobe_ADM.log C:\Program Files Creates: C:\DOCUME~1 Creates: C:\DOCUME~1\Admin Creates: C:\DOCUME~1\Admin\LOCALS~1 Creates: C:\DOCUME~1\Admin\LOCALS~1\Temp Creates: Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0 C:\Documents and Settings\Admin\Local Creates: Settings\Temp\RarSFX0__tmp_rar_sfx_access_check_86975 Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MpSvc.dll Creates: C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\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 Creates: Creates: C:\Documents and Settings Creates: C:\Documents and Settings\All Users Creates: C:\Documents and Settings\All Users\Application Data Creates: ${\tt C:\Documents\ and\ Settings\All\ Users\Application\ Data\Microsoft}$ Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync ${\tt C:\Documents\ and\ Settings\All\ Users\Application\ Data\Mozilla}$ Creates: $\hbox{C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto}\\$ Creates: $\label{lem:c:Documents} C:\Documents\ and\ Settings\All\ Users\Application\ Data\Mozilla\Crypto\RSA$ Creates: C:\Documents and Settings\All Users\Application Creates: Data\Mozilla\Crypto\RSA\MachineKeys C:\Documents and Settings\All Users\Application Creates: Data\Microsoft\DeviceSync\MsMpEng.exe Creates C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\MpSvc.dll Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\DeviceSync\delete.txt Creates: C:\Documents and Settings\All Users\Application Data\Mozilla\Crypto\RSA\MachineKeys\sgkey.data C:\Documents and Settings\All Users\Application Creates: Data\Microsoft\DeviceSync\MpSvc C:\Documents and Settings\Admin\Local Settings\Application Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB C:\Documents and Settings\All Users\Application Creates: Data\Mozilla\Crypto\RSA\MachineKeys\889EC630 Creates: C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys\5227f4c3bk Creates: C:\Documents and Settings\Admin\Local Settings\Application $\verb|DataAdobeDB90BD54-91D6-4689-A3E7-A7803574BDCB\\ \verb|warning_icon_200.png| \\$ Creates: C:\Documents and Settings\Admin\Local Settings\Application $\label{local_prop_basis} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land status_icon_caution_200.png$ C:\Documents and Settings\Admin\Local Settings\Application Creates: Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status icon caution 100.png C:\Documents and Settings\Admin\Local Settings\Application Creates: Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_125.png C:\Documents and Settings\Admin\Local Settings\Application Creates: Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_150.png

```
C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_200.png
  Creates
                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
\label{local_problem} \begin{tabular}{ll} Data \land Adobe \land DB 90BD 54 - 91D6 - 4689 - A3E7 - A7803574BDCB \land status\_icon\_x\_100.png \\ \end{tabular}
  Creates:
                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_125.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_150.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_200.png
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_100.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_125.png
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_150.png
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_darkgray_base_200.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_darkgray_base_100.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_200.png
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Application
\label{local-progress} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land progress bar\_blue\_active\_100.png
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Application
\label{local-bound} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land progressbar\_blue\_active\_125.png
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Application
{\tt Data \ Adobe \ DB90BD54-91D6-4689-A3E7-A7803574BDCB \ progress bar\_blue\_active\_150.png}
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\transparent.gif
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\gray_button_200.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\close_200.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_200.png
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_100.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_125.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_150.png
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_200.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
\label{low_button_100.png} \begin{tabular}{ll} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land yellow\_button\_100.png \\ \end{tabular}
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Application
\verb|DataAdobeDB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow\_button\_125.png|
  Creates:
                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
\verb|DataAdobeDB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow\_button\_150.png|
                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_200.png
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_100.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_125.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_150.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_200.png
  Creates:
                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_100.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_125.png
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
\label{low_button_short_150.png} \parbox{2.5cm} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land yellow\_button\_short\_150.png \parbox{2.5cm} Data \land yellow\_
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\info_icon_100.png
  Creates:
                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
Files\Content.IE5\CXCXW1MR\SC[1]
                                    C:\DOCUME~1\Admin\LOCALS~1\Temp\Adobe_ADMLogs
  Creates:
                                    C:\Documents and Settings\Admin\Local
  Creates:
Settings\Temp\Adobe_ADMLogs\Adobe_GDE.log
                                    C:\Documents and Settings\Admin\Local Settings\Application
  Creates:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\6FBB2978-428C-49A1-976F-5CC584689783
                                    C:\Documents and Settings\Admin\Cookies\admin@adobe[1].txt
  Creates:
                                    C:\Documents and Settings\Admin\Cookies\admin@adobe[2].txt
  Creates:
                                    C:\WINDOWS\Prefetch\755A4B2EC15DA6BB01248B2DFBAD2-0DD218E0.pf
  Opens:
                                    C:\Documents and Settings\Admin
  Opens:
  Opens:
                                    C:\WINDOWS\system32\winmm.dll
  Opens:
                                    C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
                                    C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
  Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
                                    C:\WINDOWS\system32\cabinet.dll
  Opens:
  Opens:
C:\WINDOWS\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
  Opens:
                                    C:\WINDOWS\system32\imm32.dll
  Opens:
                                    C:\WINDOWS\WindowsShell.Manifest
  Opens:
                                    C:\WINDOWS\WindowsShell.Config
  Opens:
                                    C:\WINDOWS\system32\shell32.dll
  Opens:
                                    C:\WINDOWS\system32\shell32.dll.124.Manifest
  Opens:
                                    C:\WINDOWS\system32\shell32.dll.124.Config
                                    C:\WINDOWS\system32\MSCTF.dll
  Opens:
```

Creates:

```
Opens:
                                      C:\WINDOWS\system32\MSCTFIME.IME
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp\$inst
  Opens:
                                     \label{local Settings-Admin-Local Settings-Temp-Sinst-2.tmp} C:\Documents and Settings-Admin-Local Settings-Temp-Sinst-2.tmp
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\7.tmp
C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\9.tmp
  Opens:
  Opens:
                                      C:\WINDOWS\system32\uxtheme.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\rpcss.dll
  Opens:
                                     C:\WINDOWS\system32\msftedit.dll
  Opens:
                                      C:\WINDOWS\win.ini
                                      C:\WINDOWS\system32\setupapi.dll
  Opens:
  Opens:
                                     C:\
  Opens:
                                     C:\WINDOWS\system32\MSIMTF.dll
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
                                      C:\Program Files\install.exe
  Opens:
                                      C:\Program Files\flashplayer18_a_install.exe
  Opens:
  Opens:
                                      C:\Program Files\Adobe\NewProduct\Uninstall.exe
                                      C:\WINDOWS\Temp\a87ac59b-3272-4219-9012-1b18fb4128b2
  Opens:
  Opens:
                                      C:\Program Files\Adobe\NewProduct
  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
  Opens:
                                      C:\Documents and Settings\All Users\Documents\desktop.ini
  Opens:
                                     C:\WINDOWS\system32\clbcatq.dll
  Opens:
                                      C:\WINDOWS\system32\comres.dll
                                      C:\WINDOWS\Registration\R000000000007.clb
  Opens:
                                      C:\WINDOWS\system32\urlmon.dll
  Opens:
                                      C:\WINDOWS\system32\urlmon.dll.123.Manifest
  Opens:
                                      C:\WINDOWS\system32\urlmon.dll.123.Config
  Opens:
  Opens:
                                      C:\WINDOWS\system32\apphelp.dll
                                      C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:
  Opens:
                                      C:\WINDOWS\AppPatch\systest.sdb
  Opens:
                                      C:\Program Files
                                     C:\Program Files\flashplayer18_a_install.exe.Manifest
C:\Program Files\flashplayer18_a_install.exe.Config
  Opens:
  Opens:
                                      C:\WINDOWS\Prefetch\FLASHPLAYER18_A_INSTALL.EXE-0B6F0919.pf
  Opens:
  Opens:
                                      C:\WINDOWS\system32\winhttp.dll
  Opens:
                                     C:\WINDOWS\system32\msi.dll
  Opens:
                                      C:\WINDOWS\system32\psapi.dll
                                      C:\WINDOWS\system32\msimg32.dll
  Opens:
  Opens:
                                      C:\WINDOWS\system32\winspool.drv
                                      C:\WINDOWS\system32\oledlg.dll
C: \verb|WINDOWS| \verb|WinSxS| x86_Microsoft. \verb|Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb54e0cdf1df_1.0.2600.5512_x-ww_dfb5
ww_dfb54e0c\GdiPlus.dll
  Opens:
                                      C:\WINDOWS\system32\crypt32.dll
  Opens:
                                     C:\WINDOWS\system32\msasn1.dll
                                     {\tt C:\WINDOWS\system32\wintrust.dll}
  Opens:
                                     C:\WINDOWS\system32\oleacc.dll
  Opens:
                                      C:\WINDOWS\system32\msvcp60.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\SHELL32.dll.124.Manifest
  Opens:
                                      C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:
                                      C:\Program Files\install.exe.Manifest
  Opens:
                                      C:\Program Files\install.exe.Config
  Opens:
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\0.tmp
  Opens:
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\1.tmp
  Opens:
                                      C:\WINDOWS\system32\oleaccrc.dll
                                      C:\WINDOWS\Prefetch\INSTALL.EXE-199863BB.pf
  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
  Opens:
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\6.tmp
  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
  Opens:
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\12.tmp
  Opens:
                                     C:\DOCUME{\sim}1\Admin\LOCALS{\sim}1\Temp\$inst\13.tmp
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\14.tmp
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\15.tmp
  Opens:
                                     C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\16.tmp
  Opens:
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\17.tmp
  Opens:
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\20.tmp
  Opens:
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\50.tmp
  Opens:
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\21.tmp
  Opens:
  Opens:
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\$inst\51.tmp
  Opens:
                                      C:\WINDOWS\system32\riched32.dll
  Opens:
                                      C:\WINDOWS\system32\riched20.dll
  Opens:
                                     C:\WINDOWS\Fonts\SEGOEUI.TTF
  Opens:
                                      C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\E431E95C-97F5-44D2-A2D6-07B00F1A955B
  Opens:
                                      C:\WINDOWS\system32\ntmarta.dll
  Opens:
                                     C:\WINDOWS\system32\samlib.dll
                                      C:\DOCUME~1\Admin\LOCALS~1\Temp\Adobe_ADMLogs\Adobe_ADM.log
  Opens:
  Opens:
                                      C:\Documents and Settings\Admin\Local
Settings\Temp\Adobe_ADMLogs\Adobe_ADM.log
  Opens:
                                     C:\Program Files\flashplayer18_a_install.exe.3.Manifest
  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\system32\ieframe.dll
  Opens:
                                      C:\Program Files\Internet Explorer\iexplore.exe
                                      C:\WINDOWS\system32\ieframe.dll.123.Manifest
  Opens:
```

```
Opens:
                          C:\WINDOWS\system32\ieframe.dll.123.Config
 Opens:
                          C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\RarSFXO}
 Opens:
                          {\tt C:\Documents\ and\ Settings\Admin\Local}
Settings\Temp\RarSFX0\
                         _tmp_rar_sfx_access_check_86975
                          C:\WINDOWS\system32\WININET.dll.123.Manifest
 Opens:
 Opens:
                          C:\WINDOWS\system32\WININET.dll.123.Config
                          {\tt C:\Documents} \ and \ {\tt Settings\Admin\Local} \ {\tt Settings\Temp\RarSFX0\MsMpEng.exe}
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Opens:
Files\Content.IE5
 Opens:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\RarSFX0\MpSvc.dll}
                          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
 Opens:
                          C:\Documents and Settings\Admin\Cookies
                          C:\Documents and Settings\Admin\Cookies\index.dat
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\RarSFX0\readme.txt}
 Opens:
 Opens:
                          C:\WINDOWS\system32\ws2_32.dll
 Opens:
                          C:\WINDOWS\system32\ws2help.dll
 Opens:
                          {\tt C:\WINDOWS\system32\mshtml.dll}
 Opens:
                          C:\WINDOWS\system32\msls31.dll
 Opens:
                          C:\Documents and Settings\Admin\Local Settings
                          C:\Documents and Settings\Admin\Local Settings\Temp
 Opens:
                          {\tt C:\Documents\ and\ Settings\backslash Admin\backslash Local\ Settings\backslash Temporary\ Internet}
 Opens:
Files\Content.IE5\QXMNQBKF
                          C:\DOCUME~1\Admin\LOCALS~1\Temp\RarSFXO\MsMpEng.exe.Manifest
 Opens
                          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:
 Opens:
                          C:\WINDOWS\system32\cryptui.dll
 Opens:
                          C:\WINDOWS\system32\CRYPTUI.dll.2.Manifest
 Opens:
                          C:\WINDOWS\system32\CRYPTUI.dll.2.Config
                          C:\WINDOWS\system32\comctl32.dll
 Opens:
                          C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
 Opens:
                          C:\WINDOWS\system32\comctl32.dll.124.Config
                          C:\WINDOWS\system32\iphlpapi.dll
 Opens:
 Opens:
                          C:\WINDOWS\system32\SHDOCVW.dll.123.Manifest
                          C:\WINDOWS\system32\SHDOCVW.dll.123.Config
  Opens:
 Opens:
                          C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync
                          C:\Documents and Settings\All Users\Application
 Opens:
Data\Microsoft\DeviceSync\MsMpEng.exe
 Opens:
                          C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\MpSvc.dll
 Opens:
                          C:\Documents and Settings\All Users\Application
Data\Mozilla\Crypto\RSA\MachineKeys
                          C:\Documents and Settings\All Users\Application
 Opens:
Data\Mozilla\Crypto\RSA\MachineKeys\sgkey.data
                          C:\WINDOWS\system32\mlang.dll
 Opens:
                          C:\WINDOWS\system32\MLANG.dll.123.Manifest
 Opens:
 Opens:
                          C:\WINDOWS\system32\MLANG.dll.123.Config
 Opens:
                          C:\WINDOWS\Prefetch\MSMPENG.EXE-1806D63D.pf
 Opens:
                          C:\WINDOWS\system32
 Opens:
                          C:\WINDOWS\system32\msxml3.dll
 Opens:
                          C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\readme.txt
                          C:\Documents and Settings\All Users\Application
.
Data\Microsoft\DeviceSync\MpSvc
                          C:\WINDOWS\system32\svchost.exe
 Opens:
 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
 Opens:
                          {\tt 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:
                          C:\WINDOWS\system32\mydocs.dll.123.Manifest
 Opens:
                          C:\WINDOWS\system32\mydocs.dll.123.Config
C:\DOCUME~1\Admin\LOCALS~1\Temp\ntshrui.dll
 Opens:
 Opens:
 Opens:
                          C:\WINDOWS\system32\ntshrui.dll
 Opens:
                          C:\WINDOWS\system32\atl.dll
 Opens:
                          C:\WINDOWS\system32\ntshrui.dll.123.Manifest
                          C:\WINDOWS\system32\ntshrui.dll.123.Config
 Opens:
 Opens:
                          C:\WINDOWS\system32\jscript.dll
 Opens:
                          C:\WINDOWS\system32\winlogon.exe
                          C:\WINDOWS\system32\xpsp2res.dll
 Opens:
                          C:\WINDOWS\system32\dxtrans.dll
 Opens:
                          C:\Documents and Settings\All Users\Application
 Opens:
Data\Mozilla\Crypto\RSA\MachineKeys\889EC630
                          C:\Documents and Settings\All Users\Application
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\ddrawex.dll
                          {\tt C:\WINDOWS\system32\mswsock.dll}
 Opens:
```

```
Opens:
                          C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                          C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS\system32\msv1_0.dll
                         C:\AUTOEXEC.BAT
 Opens:
 Opens:
                         C:\WINDOWS\system32\dllhost.exe
                         C:\WINDOWS\system32\ddraw.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\dciman32.dll
                         C:\WINDOWS\System32\dllhost.exe.Manifest
 Opens:
                         C:\WINDOWS\Prefetch\DLLHOST.EXE-45A368CC.pf
 Opens:
                         C:\WINDOWS\system32\dxtmsft.dll
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\Crypto\RSA\MachineKeys\u5227f4c3
                         C:\WINDOWS\system32\sxs.dll
 Opens:
                          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\stdole2.tlb
 Opens:
                          C:\WINDOWS\System32\TAPI32.dll.124.Manifest
 Opens:
 Opens:
                          C:\WINDOWS\System32\TAPI32.dll.124.Config
                          C:\Documents and Settings\All Users\Application
 Opens:
Data\Microsoft\Network\Connections\Pbk
 Opens:
                         C:\WINDOWS\system32\ras
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Mozilla\Firefox\profiles.ini
 Opens:
                          C:\Documents and Settings\Admin\Application
Data\Mozilla\Firefox\prefs.js
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB
                         C:\Documents and Settings\Admin\Application
 Opens
Data\Microsoft\Network\Connections\Pbk\
                         C:\WINDOWS\system32\sensapi.dll
 Opens:
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
 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:\WINDOWS\Fonts\arialbd.ttf
                          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
 Opens:
                          C:\WINDOWS\system32\TAPI32.dll.124.Manifest
                          C:\WINDOWS\system32\TAPI32.dll.124.Config
  Opens:
                         C:\WINDOWS\system32\schannel.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\dssenh.dll
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\Certificates
 Opens:
                         C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CRLs
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\SystemCertificates\My\CTLs
                         C:\Documents and Settings\Admin\Application
 Opens:
Data\Microsoft\SvstemCertificates\Mv
                         C:\WINDOWS\system32\iepeers.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\iepeers.dll.123.Manifest
                         C:\WINDOWS\system32\iepeers.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                          C:\WINDOWS\system32\imgutil.dll
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Application
 Opens:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_100.png
                          C:\WINDOWS\system32\pngfilt.dll
 Opens:
 Opens:
                          C:\Documents and Settings\Admin\Cookies\admin@adobe[1].txt
 Opens:
                          C:\Documents and Settings\Admin\Cookies\admin@adobe[2].txt
 Writes to:
                          C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
 Writes to:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\$inst\timestemp\_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
                          C:\Program Files\Adobe\NewProduct\Uninstall.ini
 Writes to:
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\Adobe_ADMLogs\Adobe_ADM.log
                         C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe
 Writes to:
                          {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\RarSFX0\MpSvc.dll}
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\readme.txt
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
 Writes to:
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
 Writes to:
                         C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\delete.txt
                          C:\Documents and Settings\All Users\Application
 Writes to:
Data\Mozilla\Crypto\RSA\MachineKeys\sgkey.data
                         C:\Documents and Settings\All Users\Application
 Writes to:
Data\Microsoft\DeviceSync\MpSvc
                         C:\Documents and Settings\All Users\Application
 Writes to:
Data\Mozilla\Crypto\RSA\MachineKeys\889EC630
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\warning_icon_200.png
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_200.png
```

```
C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_100.png
   Writes to:
                                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
\label{local-bound} \begin{tabular}{ll} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land status\_icon\_caution\_125.png \\ \begin{tabular}{ll} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land status\_icon\_caution\_125.png \\ \begin{tabular}{ll} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land status\_icon\_caution\_125.png \\ \begin{tabular}{ll} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land status\_icon\_caution\_125.png \\ \begin{tabular}{ll} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land status\_icon\_caution\_125.png \\ \begin{tabular}{ll} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land status\_icon\_caution\_125.png \\ \begin{tabular}{ll} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land status\_icon\_caution\_125.png \\ \begin{tabular}{ll} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land status\_icon\_caution\_125.png \\ \begin{tabular}{ll} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land status\_icon\_caution\_125.png \\ \begin{tabular}{ll} Data \land DB90BD54-91D6-A880-A3E7-A88035-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A880-A3E7-A
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_caution_150.png
                                                   C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_200.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_100.png
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_125.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_x_150.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_200.png
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_100.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_125.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\status_icon_check_150.png
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
\verb|DataAdobeDB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar\_darkgray\_base\_200.png|
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
\verb|DataAdobeDB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar\_darkgray\_base\_100.png|
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
\label{local_progress} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land progressbar\_blue\_active\_200.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_100.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_125.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_blue_active_150.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\transparent.gif
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\gray_button_200.png
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\close_200.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_200.png
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\progressbar_pole_null_100.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
\label{local-bound} Data \land Adobe \land DB 90BD 54 - 91D6 - 4689 - A3E7 - A7803574BDCB \land progress bar\_pole\_null\_125.png
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land progressbar\_pole\_null\_150.png
   Writes to:
                                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
\verb|DataAdobeDB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow\_button\_200.png|
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_100.png
   Writes to:
                                                   C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_125.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_150.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_200.png
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_100.png
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_125.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_mini_150.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
\label{low_button_short_200.png} \parbox{200.png} Adobe \parbox{200.png} \parbox{200.png}
   Writes to:
                                                    C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_100.png
   Writes to:
                                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
\label{low_button_short_125.png} \parbox{2.5cm} Data \land Adobe \land DB90BD54-91D6-4689-A3E7-A7803574BDCB \land yellow\_button\_short\_125.png \parbox{2.5cm} Data \land yellow\_
   Writes to:
                                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_short_150.png
                                                    C:\Documents and Settings\Admin\Local Settings\Application
   Writes to:
{\tt Data \Adobe \DB90BD54-91D6-4689-A3E7-A7803574BDCB \ info\_icon\_100.png}
                                                    \hbox{\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temporary\ Internet}
   Writes to:
Files\Content.IE5\CXCXW1MR\SC[1]
                                                   C:\Documents and Settings\Admin\Local
   Writes to:
                                          ADMLogs\Adobe_GDE.log
Settings\Temp\Adobe
                                                    C:\Documents and Settings\Admin\Cookies\admin@adobe[1].txt
   Writes to:
   Writes to:
                                                    C:\Documents and Settings\Admin\Cookies\admin@adobe[2].txt
   Reads from:
C:\WINDOWS\Temp\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
   Reads from:
                                                    C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
    Reads from
                                                    C:\WINDOWS\win.ini
   Reads from:
                                                    C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
   Reads from:
                                                    C:\Documents and Settings\Admin\My Documents\desktop.ini
   Reads from:
                                                    C:\Documents and Settings\All Users\Documents\desktop.ini
   Reads from:
                                                    C:\WINDOWS\Registration\R00000000007.clb
   Reads from:
                                                    C:\Program Files\flashplayer18_a_install.exe
   Reads from:
                                                    C:\Program Files\install.exe
   Reads from:
                                                   C:\Documents and Settings\Admin\Local
Settings\Temp\Adobe_ADMLogs\Adobe_ADM.log
   Reads from:
                                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\RarSFX0\MsMpEng.exe}
   Reads from:
                                                    {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\RarSFX0\readme.txt}
```

Writes to:

```
Reads from:
                            C:\Documents and Settings\All Users\Application
Data\Microsoft\DeviceSync\MpSvc
                           C:\Documents and Settings\All Users\Application
 Reads from:
{\tt Data\Mozilla\Crypto\RSA\Machine Keys\sgkey.data}
                           C:\Documents and Settings\All Users\Application
 Reads from:
Data\Microsoft\DeviceSync\delete.txt
 Reads from:
                           C:\AUTOEXEC.BAT
 Reads from:
                           C:\WINDOWS\system32\dxtmsft.dll
 Reads from:
                           C:\WINDOWS\system32\stdole2.tlb
                            C:\WINDOWS\system32\dxtrans.dll
  Reads from:
                            C:\WINDOWS\system32\drivers\etc\hosts
  Reads from:
                            C:\WINDOWS\system32\rsaenh.dll
  Reads from:
                            C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\Adobe_ADMLogs\Adobe_GDE.log
                            C:\WINDOWS\system32\dssenh.dll
                            C:\WINDOWS\system32\iepeers.dll
  Reads from:
                            C:\Documents and Settings\Admin\Local Settings\Application
Data\Adobe\DB90BD54-91D6-4689-A3E7-A7803574BDCB\yellow_button_100.png
  Deletes:
                            C:\Documents and Settings\Admin\Local Settings\Temp\$inst\temp_0.tmp
 Deletes:
                            C:\Documents and Settings\Admin\Local Settings\Temp\$inst\2.tmp
  Deletes:
                            {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\$inst}\\
 Deletes:
                            {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Application}
Data\Adobe\E431E95C-97F5-44D2-A2D6-07B00F1A955B
 Deletes:
                           C:\Documents and Settings\Admin\Local
{\tt Settings\Temp\RarSFX0\\_tmp\_rar\_sfx\_access\_check\_86975}
  Deletes:
                            C:\Program Files\install.exe
                            C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MpSvc.dll C:\Documents and Settings\Admin\Local Settings\Temp\RarSFX0\MsMpEng.exe
  Deletes:
 Deletes:
                            C:\Documents and Settings\Admin\Local Settings\Temp\RarSFXO\readme.txt
C:\Documents and Settings\Admin\Local Settings\Temp\RarSFXO
 Deletes:
 Deletes:
                            C:\Documents and Settings\All Users\Application
 Deletes:
Data\Microsoft\DeviceSync\delete.txt
                            C:\Documents and Settings\Admin\Cookies\admin@adobe[1].txt
 Deletes:
```

Network Events

DNS query:	linuxdns.sytes.net
DNS query:	get.adobe.com
DNS query:	systeminfothai.gotdns.ch
DNS query:	sysnc.sytes.net
DNS query:	dlmping2.adobe.com
DNS query:	stats.adobe.com
DNS response:	linuxdns.sytes.net ⇒ 0.0.0.0
DNS response:	get.wip4.adobe.com ⇒ 193.104.215.66
DNS response:	systeminfothai.gotdns.ch \Rightarrow 0.0.0.0
DNS response:	sysnc.sytes.net ⇒ 0.0.0.0
DNS response:	e4578.g.akamaiedge.net ⇒ 118.214.80.175
DNS response:	adobe.com.d1.sc.omtrdc.net \Rightarrow 192.243.250.16
DNS response:	adobe.com.d1.sc.omtrdc.net ⇒ 192.243.250.65
Connects to:	0.0.0:80
Connects to:	127.0.0.1:1048
Connects to:	0.0.0.0:1433
Connects to:	0.0.0:8080
Connects to:	0.0.0:53
Connects to:	0.0.0:443
Connects to:	193.104.215.66:443
Connects to:	0.0.0.0:21
Connects to:	127.0.0.1:1121
Connects to:	127.0.0.1:1138
Connects to:	118.214.80.175:443
Connects to:	192.243.250.16:80
Sends data to:	8.8.8.8:53
Sends data to:	127.0.0.1:1048
Sends data to:	get.wip4.adobe.com:443 (193.104.215.66)
Sends data to:	127.0.0.1:1121
Sends data to:	e4578.g.akamaiedge.net:443 (118.214.80.175)
Sends data to:	127.0.0.1:1138
Sends data to:	adobe.com.d1.sc.omtrdc.net:80 (192.243.250.16)
Receives data from:	sysnc.sytes.net:0 (0.0.0.0)
Receives data from:	get.wip4.adobe.com:443 (193.104.215.66)
Receives data from:	e4578.g.akamaiedge.net:443 (118.214.80.175)
Receives data from:	127.0.0.1:1138
Receives data from:	adobe.com.d1.sc.omtrdc.net:80 (192.243.250.16)

Windows Registry Events		
Creates key:		
HKCU\software\micro	osoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-	
806d6172696f}\		
Creates key:	<pre>HKLM\software\microsoft\windows\currentversion\uninstall\newproduct 1.00</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\user shell</pre>	
folders		
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\shell folders</pre>	
Creates key:	<pre>HKLM\software\microsoft\windows\currentversion\explorer\user shell</pre>	
folders		
Creates key:	<pre>HKLM\software\microsoft\windows\currentversion\explorer\shell folders</pre>	
Creates key:	<pre>HKLM\software\microsoft\windows\currentversion\shell extensions\blocked</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\shell extensions\blocked</pre>	
Creates key:	<pre>HKLM\software\microsoft\windows\currentversion\shell extensions\cached</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\shell extensions\cached</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings</pre>	
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\explorer\userassist</pre>	
Creates key:		
HKCU\software\micro	osoft\windows\currentversion\explorer\userassist\{75048700-ef1f-11d0-9888-	

```
006097deacf93
     Creates key:
HKCU \setminus software \setminus irrosoft \setminus ir
006097deacf9}\count
    Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{5e6ab780-7743-11cf-a12b-
00aa004ae837}
    Creates kev:
00aa004ae837}\count
     Creates key:
                                                                          HKLM\software\classes
     Creates key:
                                                                          HKU\.default\software\microsoft\windows\currentversion\internet settings
     Creates key:
                                                                          HKU\.default\software\microsoft\multimedia\audio
     Creates key:
                                                                          HKU\.default\software\microsoft\multimedia\audio compression manager\
     Creates key:
                                                                          HKU\.default\software\microsoft\multimedia\audio compression
manager\msacm
                                                                          HKU\.default\software\microsoft\multimedia\audio compression
    Creates key:
manager\priority v4.00
     Creates key:
                                                                          HKU\s-1-5-21-1757981266-507921405-1957994488-
 1003\software\microsoft\windows nt\currentversion\winlogon
     Creates key:
                                                                          {\tt HKLM \backslash software \backslash microsoft \backslash direct draw \backslash most recent application}
     Creates key:
                                                                          HKCU\software\microsoft\multimedia\audio
     Creates key:
                                                                          HKCU\software\microsoft\multimedia\audio compression manager\
    Creates key:
                                                                          HKCU\software\microsoft\multimedia\audio compression manager\msacm
    Creates key:
                                                                          \label{lem:hkcu} \verb+KKCU\software\microsoft\multimedia\audio compression manager\microsoft\multimedia\audio compression manager\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsof
v4.00
                                                                          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
                                                                          HKLM\software\microsoft\tracing
     Creates key:
                                                                          HKU\s-1-5-21-1757981266-507921405-1957994488-
     Creates key:
1003\software\microsoft\windows\currentversion\internet settings\connections
    Creates kev:
                                                                          HKU\s-1-5-21-1757981266-507921405-1957994488-
 1003\software\microsoft\windows\currentversion\internet settings
                                                                         HKU\s-1-5-21-1757981266-507921405-1957994488-
    Creates key:
 1003\software\microsoft\windows nt\currentversion\network\location awareness
     Creates kev:
                                                                          HKLM\system\currentcontrolset\services\tcpip\parameters
     Creates key:
                                                                          HKCU\software\microsoft\windows script\settings
                                                                          HKCU\software\microsoft\windows\currentversion\wintrust\trust
     Creates key:
providers\software publishing
                                                                          HKCU\software\microsoft\systemcertificates\root
     Creates key:
     Creates key:
                                                                          HKCU\software\microsoft\systemcertificates\root\certificates
     Creates key:
                                                                          HKCU\software\microsoft\systemcertificates\root\crls
     Creates key:
                                                                          HKCU\software\microsoft\systemcertificates\root\ctls
     Creates key:
                                                                          {\it HKLM} \ software \ `microsoft \ 'system certificates \ 'root
     Creates key:
                                                                          {\tt HKLM \backslash software \backslash microsoft \backslash system} certificates \backslash root \backslash crls
     Creates key:
    Creates kev:
                                                                          {\it HKLM \ } software \verb|\microsoft \ system certificates \verb|\noot \ ctls| \\
     Creates key:
                                                                          {\tt HKLM \backslash software \backslash microsoft \backslash system certificates \backslash authroot}
     Creates key:
                                                                          HKLM \setminus software \setminus microsoft \setminus system certificates \setminus authroot \setminus certificates
     Creates kev:
                                                                          HKLM\software\microsoft\systemcertificates\authroot\crls
                                                                          HKLM\software\microsoft\systemcertificates\authroot\ctls
    Creates kev:
                                                                          HKLM\software\policies\microsoft\systemcertificates\root
     Creates kev:
    Creates key:
                                                                          HKLM\software\policies\microsoft\systemcertificates\root\certificates
     Creates key:
                                                                          HKLM\software\policies\microsoft\systemcertificates\root\crls
    Creates key:
                                                                          HKLM\software\policies\microsoft\systemcertificates\root\ctls
     Creates key:
                                                                          HKLM\software\microsoft\enterprisecertificates\root
     Creates key:
                                                                          HKLM\software\microsoft\enterprisecertificates\root\certificates
     Creates key:
                                                                          HKLM\software\microsoft\enterprisecertificates\root\crls
                                                                          Creates key:
                                                                          \label{prop:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \system certificates \cal{lkcu} \\ \end{tabular}
     Creates key:
     Creates key:
                                                                          \begin{tabular}{ll} HKCU \software \mbox{$^$ is system certificates} \calcertificates \end{tabular} \label{table}
     Creates key:
                                                                          HKCU\software\microsoft\systemcertificates\ca\crls
     Creates key:
                                                                          HKCU\software\microsoft\systemcertificates\ca\ctls
     Creates key:
                                                                          HKCU\software\policies\microsoft\systemcertificates\ca
     Creates key:
                                                                          HKCU\software\policies\microsoft\systemcertificates\ca\certificates
     Creates key:
                                                                          HKCU\software\policies\microsoft\systemcertificates\ca\crls
     Creates key:
                                                                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \system certificates \ca\ctls \end{tabular}
    Creates kev:
                                                                          {\it HKLM} \ software \ `microsoft\ 'system certificates \ `ca\ 'certificates' \ 'all \ 'system' \ 'all \ 'system' \ 'all \ 'all
     Creates kev:
     Creates key:
                                                                          HKLM\software\microsoft\systemcertificates\ca\crls
                                                                          HKLM\software\microsoft\systemcertificates\ca\ctls
     Creates key:
                                                                          HKLM\software\policies\microsoft\systemcertificates\ca
     Creates key:
                                                                          HKLM\software\policies\microsoft\systemcertificates\ca\certificates
     Creates key:
                                                                          HKLM\software\policies\microsoft\systemcertificates\ca\crls
     Creates key:
     Creates key:
                                                                          HKLM\software\policies\microsoft\systemcertificates\ca\ctls
    Creates key:
                                                                          HKLM\software\microsoft\enterprisecertificates\ca
     Creates key:
                                                                          HKLM\software\microsoft\enterprisecertificates\ca\certificates
     Creates key:
                                                                          HKLM\software\microsoft\enterprisecertificates\ca\crls
     Creates key:
                                                                          HKLM\software\microsoft\enterprisecertificates\ca\ctls
     Creates key:
                                                                          {\tt HKCU \backslash software \backslash microsoft \backslash system} \\ \dot{\text{constant}} \\ \dot{\text{constant
     Creates key:
                                                                          HKCU \setminus software \setminus microsoft \setminus system certificates \setminus disallowed \setminus certificates
                                                                          HKCU\software\microsoft\systemcertificates\disallowed\crls
     Creates key:
                                                                          HKCU\software\microsoft\systemcertificates\disallowed\ctls
     Creates key:
     Creates key:
                                                                          HKCU\software\policies\microsoft\systemcertificates\disallowed
     Creates key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus disallowed \setminus certificates
     Creates key:
                                                                          HKCU\software\policies\microsoft\systemcertificates\disallowed\crls
      Creates key:
                                                                          HKCU \ software \ policies \ microsoft \ system certificates \ disallowed \ ctls
     Creates key:
                                                                          {\tt HKLM \setminus software \setminus microsoft \setminus system certificates \setminus disallowed}
     Creates key:
                                                                          HKLM \verb|\software\m| icrosoft \verb|\systemcertificates\m| disallowed \verb|\certificates\m|
```

 $\label{thm:hklmsoftware\microsoft} HKLM \noindent \noi$

Creates key:

Creates key:

```
Creates key:
                                                                      HKLM\software\policies\microsoft\systemcertificates\disallowed
     Creates key:
HKLM \verb|\software\policies\m| icrosoft \verb|\systemcertificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\certificates\allowed\ce
     Creates key:
                                                                     {\tt HKLM \ } software \verb|\ policies \verb|\ microsoft \ | system certificates \verb|\ disallowed \ | crls
     Creates key:
                                                                     HKLM\software\policies\microsoft\systemcertificates\disallowed\ctls
                                                                      HKLM\software\microsoft\enterprisecertificates\disallowed
     Creates kev:
    Creates key:
                                                                     HKLM \setminus software \setminus microsoft \setminus enterprise certificates \setminus disallowed \setminus certificates
     Creates kev:
                                                                      HKLM\software\microsoft\enterprisecertificates\disallowed\crls
     Creates key:
                                                                      Creates key:
                                                                      HKCU\software\microsoft\systemcertificates\trust
     Creates key:
                                                                      \begin{tabular}{ll} HKCU \label{linear} \textbf{KCU} \label{linear} \textbf{Software} \end{tabular} \vec{\textbf{MKCU}} \end{tabular} \vec{\textbf{Software}} \vec{\textbf{MKCU}} \vec{\textbf{Software}} \vec{\textbf{MKCU}} \vec{\textbf{Software}} \vec{\textbf{MKCU}} \vec{\textbf{MCU}} \vec{\textbf{MCCU}} \vec{\textbf{MC
     Creates key:
                                                                      HKCU\software\microsoft\systemcertificates\trust\crls
     Creates key:
                                                                      HKCU\software\microsoft\systemcertificates\trust\ctls
     Creates key:
                                                                      HKCU\software\policies\microsoft\systemcertificates\trust
     Creates key:
                                                                      HKCU\software\policies\microsoft\systemcertificates\trust\certificates
     Creates key:
                                                                      HKCU\software\policies\microsoft\systemcertificates\trust\crls
     Creates key:
                                                                      HKCU\software\policies\microsoft\systemcertificates\trust\ctls
     Creates key:
                                                                      HKLM\software\microsoft\systemcertificates\trust
                                                                      HKLM\software\microsoft\systemcertificates\trust\certificates
     Creates key:
     Creates key:
                                                                      HKLM\software\microsoft\systemcertificates\trust\crls
                                                                      {\tt HKLM \ } software \verb|\ microsoft \ | system certificates \verb|\ trust \ | ctls \\
     Creates key:
     Creates key:
                                                                      HKLM\software\policies\microsoft\systemcertificates\trust
     Creates key:
                                                                      HKLM\software\policies\microsoft\systemcertificates\trust\certificates
     Creates key:
                                                                      Creates key:
                                                                      Creates key:
                                                                      HKLM\software\microsoft\enterprisecertificates\trust
     Creates key:
                                                                      Creates key:
                                                                      HKLM\software\microsoft\enterprisecertificates\trust\crls
                                                                      Creates key:
                                                                      HKCU\software\microsoft\systemcertificates\my
     Creates key:
     Creates key:
                                                                      HKCU\software\microsoft\windows nt\currentversion\winlogon
     Creates key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25
                                                                     HKCU\software\microsoft\windows\currentversion\internet
    Creates kev:
settings\connections
    Creates key:
                                                                      HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
    Creates key:
                                                                      HKCU\software\microsoft\windows\currentversion\internet
 settings\p3p\history
                                                                      HKU\s-1-5-21-1757981266-507921405-1957994488-
     Deletes value:
 1003\software\microsoft\windows\currentversion\internet settings[proxyserver]
                                                                      HKU\s-1-5-21-1757981266-507921405-1957994488-
     Deletes value:
 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]
    Deletes value:
HKLM \label{lem:hklm} Which is the lemma of the lemma o
    Deletes value:
                                                                      HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
    Deletes value:
                                                                      HKCU\software\microsoft\windows\currentversion\internet
 settings[proxyoverride]
    Deletes value:
                                                                      HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
                                                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens kev:
options\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
                                                                     HKLM\system\currentcontrolset\control\terminal server
     Opens key:
     Opens key:
                                                                     HKLM\system\currentcontrolset\control\safeboot\option
                                                                      HKLM\software\policies\microsoft\windows\safer\codeidentifiers
     Opens key:
                                                                     HKCU\software\policies\microsoft\windows\safer\codeidentifiers
     Opens key:
     Opens key:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} idebyside \end{tabular} assembly storage roots
    Opens key:
                                                                      \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\gdi32.dll
     Opens key:
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
     Opens key:
                                                                      HKLM\system\currentcontrolset\control\session manager
     Opens key:
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
    Opens key:
                                                                      \label{lem:hklm} \mbox{HKLM\software\mbox{$\backslash$ microsoft\windows nt\currentversion\selection}} \ \ \mbox{microsoft\windows nt\currentversion\selection} \ \ \mbox{\selection} \ \ \mbox{\selection} \ \mbox{\
options\ntdll.dll
     Opens key:
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
    Opens key:
                                                                      \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ 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
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options\msvcrt.dll
    Opens key:
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options\oleaut32.dll
     Opens key:
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens key:
options\shlwapi.dll
     Opens key:
                                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\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
   Opens key:
                                              \label{lem:hklm} \verb+Kklm\+ software\+ initialize+ of the limits of the 
   Opens key:
                                              {\tt HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus compatibility 32}
   Opens kev:
                                              HKLM\software\microsoft\windows nt\currentversion\ime compatibility
   Opens kev:
                                              HKLM\software\microsoft\windows nt\currentversion\windows
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\winlogon
                                              HKLM\
   Opens kev:
                                              HKLM\software\microsoft\windows nt\currentversion\diagnostics
   Opens key:
                                              HKLM\software\microsoft\ole
   Opens kev:
   Opens key:
                                              HKCR\interface
   Opens key:
                                              HKCR\interface\{00020400-0000-0000-c000-000000000046}
   Opens key:
                                              HKLM\software\microsoft\oleaut
   Opens key:
                                              HKLM\software\microsoft\oleaut\userera
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\drivers32
   Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
                                              HKLM\software\microsoft\windows\currentversion\explorer\performance
   Opens kev:
   Opens key:
   Opens key:
                                              HKCU\software\policies\microsoft\control panel\desktop
   Opens key:
                                              HKCU\control panel\desktop
   Opens key:
                                              \label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\advanced
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\languagepack
   Opens key:
                                              HKLM\system\setup
   Opens key:
                                              \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\msctf.dll
   Opens key:
Opens key:
                                              HKLM\software\microsoft\ctf\systemshared\
                                              HKCU\keyboard layout\toggle
   Opens key
   Opens key:
                                              HKLM\software\microsoft\ctf\
                                              HKLM\software\microsoft\windows nt\currentversion\imm
   Opens key:
   Opens kev:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
                                              HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
   Opens kev:
   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 kev:
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
   Opens key:
                                              \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+theme manager
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msftedit.dll
   Opens key:
                                              HKCU\software\microsoft\windows nt\currentversion\windows
   Opens key:
                                              HKLM\software\microsoft\windows
\verb|nt\current| version \verb|\language| pack \verb|\surrogatefall| back|
   Opens key:
                                              HKLM\software\microsoft\windows\currentversion\explorer\advanced
   Opens key
                                              HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
   Opens key:
                                              HKLM\software\microsoft\windows\currentversion
                                              HKLM\software\microsoft\windows\currentversion\policies\explorer
   Opens kev:
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\policies\explorer
   Opens kev:
HKLM\software\microsoft\windows\currentyersion\shellcompatibility\applications\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe
   Opens kev:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-
a2d8-08002b30309d}
                                              HKCU\software\classes\
   Opens key:
   Opens key
                                              HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
                                              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\nprocserver 32
   Opens key:
                                              {\tt HKLM \ }. \\
   Opens key:
options\setupapi.dll
                                              HKLM\system\currentcontrolset\control\minint
   Opens key:
   Opens key:
                                              HKLM\system\wpa\pnp
   Opens key:
                                              HKLM\software\microsoft\windows\currentversion\setup
   Opens key:
                                              HKLM\software\microsoft\windows\currentversion\setup\apploglevels
   Opens key:
                                              HKLM \verb|\system| current controlset \verb|\control| computer name \verb|\activecomputer name| active computer name \verb|\control| computer name active computer name \verb|\control| computer name active name active computer name active name
   Opens key:
                                              {\it HKLM} \verb|\system| current control set \verb|\services| tcpip \verb|\parameters| \\
   Opens key:
                                              HKLM\software\policies\microsoft\system\dnsclient
   Opens key:
                                              HKLM \verb|\software\microsoft\pc\pagedbuffers|
                                              HKLM\software\microsoft\rpc
   Opens kev:
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe\rpcthreadpoolthrottle
                                              HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
   Opens key
                                              HKLM\system\currentcontrolset\control\computername
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
   Opens key:
11e3-9fc7-806d6172696f}\
   Opens key:
                                              HKCU\software\classes\directory
   Opens key:
                                              HKCR\directory
                                              HKCU\software\classes\directory\curver
   Opens key:
   Opens key:
                                              HKCR\directory\curver
   Opens key:
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\explorer
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\explorer\
   Opens key:
                                              HKCU\software\microsoft\windows\currentversion\policies\system
   Opens key:
                                              HKCU\software\classes\directory\shellex\iconhandler
   Opens key:
                                              HKCR\directory\shellex\iconhandler
   Opens key:
                                              HKCU\software\classes\directory\clsid
```

Opens key:

HKCR\directory\clsid
HKCU\software\classes\folder

```
Opens key:
                                                               HKCR\folder
    Opens key:
                                                               HKCU\software\classes\folder\clsid
    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
                                                               HKCU\software\classes\drive\shellex\folderextensions
    Opens key:
    Opens kev:
                                                               HKCR\drive\shellex\folderextensions
Opens key:
4442-804e-409d6c4515e9}
                                                               HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
    Opens key:
                                                               HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\fileexts
    Opens key:
                                                               HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe
    Opens key:
                                                               HKCU\software\classes\.exe
    Opens key:
                                                               HKCR\.exe
                                                               HKCU\software\classes\exefile
    Opens key:
    Opens kev:
                                                               HKCR\exefile
                                                               HKCU\software\classes\exefile\curver
    Opens key:
    Opens key:
                                                               HKCR\exefile\curve
                                                               HKCR\exefile\
    Opens key:
    Opens key:
                                                               HKCU\software\classes\exefile\shellex\iconhandler
    Opens key:
                                                               HKCR\exefile\shellex\iconhandler
    Opens key:
                                                               HKCU\software\classes\systemfileassociations\.exe
    Opens key:
                                                               HKCR\systemfileassociations\.exe
    Opens key:
                                                               HKCU\software\classes\systemfileassociations\application
    Opens key:
                                                               {\it HKCR} \verb|\systemfile| associations \verb|\application| \\
    Opens key:
                                                               HKCU\software\classes\exefile\clsid
    Opens key:
                                                               HKCR\exefile\clsid
                                                               HKCU\software\classes\*
    Opens key:
                                                               HKCR\*
    Opens key:
                                                               HKCU\software\classes\*\clsid
    Opens key:
    Opens kev:
                                                               HKCR\*\clsid
    Opens kev:
HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks
                                                              HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-
    Opens key:
00c04fd91972}\inprocserver32
                                                               HKCR\clsid\\\{aeb6717e-7e19-11d0-97ee-00c04fd91972\\\}\inprocserver32
    Opens key:
    Opens kev:
                                                               HKLM\software\microsoft\windows\currentversion\policies\associations
    Opens key:
                                                               {\tt HKCU \ } . \\ {\tt KCU \ } . \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash associations \\ {\tt Current \ } version \backslash policies \backslash policies \backslash policies \backslash policies \backslash policies \backslash policies \\ {\tt Current \ } version \backslash policies \backslash 
    Opens key:
                                                               HKCU\software\classes\.ade
    Opens key:
                                                               HKCR\.ade
    Opens key:
                                                               HKCU\software\classes\.adp
    Opens key:
                                                               HKCR\.adp
    Opens key:
                                                               HKCU\software\classes\.app
    Opens key:
                                                               HKCR\.app
    Opens key:
                                                               HKCU\software\classes\.asp
    Opens key:
                                                               HKCR\.asp
    Opens key:
                                                               HKCU\software\classes\.bas
    Opens key:
                                                               HKCR\.bas
                                                               HKCU\software\classes\.bat
    Opens key:
    Opens key:
                                                               HKCR\.bat
                                                               HKCU\software\classes\.cer
    Opens key:
                                                               HKCR\.cer
    Opens kev:
                                                               HKCU\software\classes\.chm
    Opens kev:
    Opens key:
                                                               HKCR\.chm
    Opens key:
                                                               HKCU\software\classes\.cmd
                                                               HKCR\.cmd
    Opens key:
    Opens key:
                                                               HKCU\software\classes\.com
    Opens key:
                                                               HKCR\.com
                                                               HKCU\software\classes\.cpl
    Opens key:
    Opens key:
                                                               HKCR\.cpl
    Opens key:
                                                               HKCU\software\classes\.crt
    Opens key:
                                                               HKCR\.crt
    Opens key:
                                                               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
                                                               HKLM\software\microsoft\com3\debug
    Opens key:
                                                               HKLM\software\classes
    Opens key:
    Opens key:
                                                               HKU\
                                                               HKCR\clsid
    Opens key:
    Opens key:
                                                               HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
                                                               HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
    Opens key:
                                                               HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
    Opens key:
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 \c1sid \f3b8a2d94-0ac9-11d1-896c-00c04fb6bfc4 \nprocserver 32
    Opens key:
    Opens key:
                                                               HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserverx86
    Opens key:
                                                               HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid
                                                               HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
    Opens key:
```

00c04fb6bfc4}\localserver32

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

Opens key: 00c04fb6bfc4}\inprochandler32

Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32

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

00c04fb6bfc4}\inprochandlerx86

```
Opens key:
                                                           HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\tinprochandlerx86
   Opens key:
                                                          HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\localserver
   Opens key:
                                                           HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver
   Opens kev:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
   Opens key:
                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
   Opens key:
                                                           HKCU\software\classes\protocols\name-space handler\
   Opens key:
                                                           HKCR\protocols\name-space handler
   Opens key:
                                                           HKCU\software\classes\protocols\name-space handler
   Opens key:
                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
settings
   Opens key:
                                                           HKLM\software\microsoft\windows\currentversion\internet settings
   Opens key:
                                                           HKLM\software\policies\microsoft\windows\currentversion\internet
settings
   Opens key:
                                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
                                                          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:
                                                          \label{lem:hkcu} \verb+KKCU\+ software \verb+\policies+ microsoft+ internet explorer+ main+ feature control
   Opens key:
                                                           HKLM\software\microsoft\internet explorer\main\featurecontrol
   Opens key
                                                           HKCU\software\microsoft\internet explorer\main\featurecontrol
   Opens key:
                                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
   Opens key:
                                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature ignore policies zonemap if esc enabled kb918915
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens key:
settings\zonemap\domains\
   Opens kev:
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\ranges\
   Opens key:
                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
   Opens key:
                                                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
   Opens key:
                                                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
   Opens key:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
                                                           HKCU\software\microsoft\internet
   Opens key:
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 kev:
                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                                                          HKCU\software\microsoft\windows\currentversion\internet
   Opens kev:
settings\zonemap\protocoldefaults\
   Opens key:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
   Opens key:
                                                          HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
   Opens key:
                                                          HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com
                                                          HKLM\software\microsoft\windows\currentversion\internet
   Opens key:
settings\zonemap\domains\msn.com\related
   Opens key:
                                                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
                                                          HKLM\software\microsoft\internet
   Opens key:
explorer \verb|\main| featurecontrol| feature\_use\_ietldlist\_for\_domain\_determination| featurecontrol| feature\_use\_ietldlist\_for\_domain\_determination| featurecontrol| featurecon
   Opens key:
                                                           HKCU\software\microsoft\internet explorer\ietld
   Opens key:
                                                          HKCU\software\microsoft\internet
\verb|explorer| main feature control feature initialize urlaction_shell execute to allow kb936610| feature featu
   Opens kev:
                                                          HKLM\software\microsoft\internet
\verb|explorer| main feature control feature initialize urlaction_shell execute_to_allow_kb936610| | the feature feature
   Opens key
                                                           HKCU\software\microsoft\windows\currentversion\internet settings
   Opens key:
                                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature http username password disable
   Opens key:
                                                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
                                                           HKCU\software\microsoft\internet
   Opens key:
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 kev:
                                                           HKLM\software\policies\microsoft\internet explorer\security
```

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\

HKCU\software\microsoft\windows\currentversion\internet settings\zones\

HKCU\software\microsoft\windows\currentversion\internet settings\zones\0

Opens key:

```
Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
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
  Opens key:
                                      \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \normalisation \normalisatio
settings\zones\3
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
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
\verb|explorer\main\featurecontrol\feature_localmachine_lockdown|
                                      HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
  Opens key
settings\lockdown_zones\
  Opens key
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
\verb|settings\lockdown_zones||
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown zones\
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\0
  Opens kev:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\0
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\0
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\1
  Opens kev:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:
                                      \label{lem:hkcu} \verb+KKCU \software \policies \microsoft \windows \current version \current \end{tensor} \\
settings\lockdown zones\1
  Opens key
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
                                      \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\2
  Opens key
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\2
  Opens key
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\3
  Opens key
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                      \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}
  Opens kev:
settings\lockdown zones\3
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\4
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown zones\4
  Opens key
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
                                      HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:
                                      HKCU\software\classes\exefile\shell\open
  Opens key:
                                      HKCR\exefile\shell\open
  Opens key:
                                      HKCU\software\classes\exefile\shell\open\command
  Opens key:
                                      HKCR\exefile\shell\open\command
  Opens key:
\label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ policies \+ explorer \+ restrict run
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\app
paths\flashplayer18_a_install.exe
  Opens key:
                                      HKCU\software\classes\exefile\shell\open\ddeexec
  Opens key:
                                      HKCR\exefile\shell\open\ddeexec
  Opens key:
                                      HKCU\software\classes\applications\flashplayer18 a install.exe
  Opens key:
                                      HKCR\applications\flashplayer18_a_install.exe
                                      HKCU\software\microsoft\windows\shellnoroam
  Opens key:
                                      HKCU\software\microsoft\windows\shellnoroam\muicache
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\windows\shellnoroam\muicache\
  Opens key:
                                      HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
  Opens key:
                                      HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:
                                      HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
  Opens key:
                                      HKLM\system\wpa\tabletpc
   Opens key:
                                      HKLM\system\wpa\mediacenter
                                      HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:
  Opens key:
                                      HKLM\software\microsoft\windows
\verb|nt\currentversion\appcompatflags\custom\flashplayer18\_a\_install.exe|
  Opens key:
                                      HKLM\software\policies\microsoft\windows\safer\levelobjects
  Opens key
                                      HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus paths
  Opens key:
```

be2efd2c1a33}

```
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
     Opens key:
     Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{349d35ab-37b5-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-462f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-4666f-9b89-46666f-9b89-4666
edd5fbde1328}
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb913
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f3
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
     Opens key:
b91490411bfc}
     Opens key:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 0 \ vert zones
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
     Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus has hes \in microsoft \setminus microsoft \setminus has held in the policies \setminus has held
     Opens key:
HKLM \verb|\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
     Opens key
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus paths
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
     Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
     Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
     Opens key:
HKLM\software\policies\microsoft\windows\safer\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
     Opens key:
                                                                              HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
     Opens key:
                                                                              \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \node \node
     Opens key:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \parbox{0.4cm} urlzones \parbox{0.4cm} and \parbox{0.4cm
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
     Opens key
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
     Opens key
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
     Opens key
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
     Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus has hes
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
     Opens key:
HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus has hes
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
     Opens key:
                                                                              HKCU\software\microsoft\windows\currentversion\explorer\shell folders
     Opens key
                                                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\flashplayer18_a_install.exe
     Opens key:
                                                                             HKLM\software\microsoft\windows\currentversion\app paths\install.exe
     Opens key:
                                                                              HKCU\software\classes\applications\install.exe
                                                                             HKCR\applications\install.exe
     Opens key:
     Opens key:
                                                                             HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\install.exe
                                                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens key:
options\winhttp.dll
                                                                             HKLM\software\microsoft\windows\currentversion\internet
     Opens key:
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 key:
                                                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msimg32.dll
     Opens key:
                                                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\winspool.drv
     Opens key
                                                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\oledlg.dll
     Opens key:
                                                                              HKCU\software\classes\clsid
```

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

```
options\gdiplus.dll
    Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe
   Opens key:
                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens kev:
options\crypt32.dll
   Opens key:
                                                       HKLM\system\currentcontrolset\services\crypt32\performance
    Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\msasn1
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\imagehlp.dll
   Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wintrust.dll
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\mpr.dll
    Opens key:
                                                       {\tt HKLM \ } system \verb|\ current control \ $$ et \ \ $$ in the two rkprovider \verb|\ hworder \ \ $$ et \ \ $$ in the two rkprovider \ \ $$ et \ \ \ $$ et \ \ $$ et \ \ $
    Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp60.dll
    Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleacc.dll
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options\comdlg32.dll
    Opens key:
                                                       HKLM\software\microsoft\ctf\compatibility\install.exe
   Opens key:
                                                       \label{lem:hklm} \mbox{HKLM\software\mbox{$\backslash$ microsoft\windows nt\currentversion\selection}} \ \ \mbox{microsoft\windows nt\currentversion\selection} \ \ \mbox{\selection} \ \ \mbox{\selection} \ \mbox{\
options\riched20.dll
    Opens key
                                                       \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\riched32.dll
    Opens key
                                                       HKCU\software\microsoft\windows\currentversion\policies\network
    Opens key:
                                                       HKCU\software\microsoft\windows\currentversion\policies\comdlg32
                                                       HKLM\software\microsoft\ctf\compatibility\flashplayer18_a_install.exe
    Opens key:
   Opens key:
                                                       HKLM\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 key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntmarta.dll
    Opens key:
                                                       HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
                                                       HKLM\software\microsoft\windows\currentversion\explorer\autocomplete
    Opens kev:
    Opens key:
                                                       HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
    Opens key:
                                                       HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}
                                                       Opens key:
00c04fd7d062}\treatas
                                                       \label{localization} HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\ \ treat as
    Opens key:
    Opens key
                                                      HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
    Opens key:
                                                      HKCR \ clsid \ \{00bb2765-6a77-11d0-a535-00c04fd7d062\} \ \ inprocserver 32
    Opens key
                                                      00c04fd7d062}\inprocserverx86
    Opens key:
                                                      HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
    Opens key
                                                      HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535
00c04fd7d062}\localserver32
                                                      HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\localserver32
    Opens key:
                                                      HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
   Opens key
00c04fd7d062}\inprochandler32
                                                      HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandler32
    Opens key:
   Opens key
                                                      HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprochandlerx86
                                                      HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86
    Opens key:
    Opens key
                                                      HKCU\software\classes\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\localserver
    Opens key:
                                                      Opens key:
                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{8856f961-340a-11d0-a96b-00c04fd705a2\}
                                                       HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
    Opens key:
                                                       HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
    Opens key:
00c04fd705a2}\treatas
                                                       HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
    Opens key:
    Opens key
                                                      HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
    Opens key:
                                                      HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
    Opens key:
                                                      HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
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
                                                      HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
   Opens key:
00c04fd705a2}\inprochandler32
                                                      HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler 32
    Opens key:
                                                      HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
    Opens key
00c04fd705a2}\inprochandlerx86
                                                      HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx86
    Opens key:
    Opens key:
                                                      HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\localserver
   Opens key:
                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\browseui.dll
                                                       HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver
    Opens key:
    Opens key:
                                                      HKCU \setminus software \setminus classes \setminus clsid \setminus \{03c036f1-a186-11d0-824a-00aa005b4383\}
                                                      HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}
    Opens key:
    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 \setminus software \setminus classes \setminus clsid \setminus \{03c036f1-a186-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d0-824a-11d
00aa005b4383}\inprocserver32
```

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

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

00aa005b4383}\inprocserverx86

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

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

00aa005b4383}\localserver32

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

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

00aa005b4383}\inprochandler32

HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandler32 Opens kev:

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

00aa005b4383}\inprochandlerx86

Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandlerx86 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\ieframe.dll

Opens key: $\label{lem:hklm} \verb+Kklm/software/microsoft/windows/currentversion/app paths/iexplore.exe$

Opens key: HKLM\software\microsoft\internet explorer\setup HKLM\system\currentcontrolset\control\wmi\security Opens key HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-Opens key

00aa005b4383}\localserver

Opens key: HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver Opens key $HKCU \setminus software \setminus classes \setminus clsid \setminus \{00bb2763-6a77-11d0-a535-00c04fd7d062\}$ 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\interface\{eab22ac1-30c1-11cf-a7eb-Opens key:

0000c05bae0b}\typelib

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

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

00aa00404770}\proxystubclsid32

Opens key: $HKCR \land eface \land \{b722bccb-4e68-101b-a2bc-00aa00404770\} \land proxystubclsid 32$

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

00c04fd7d062}\inprocserverx86

 $HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\tinprocserverx86$ Opens key:

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

00c04fd7d062}\localserver32

Opens key HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver32 HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c82-Opens key

00aa004ba90b}\proxystubclsid32

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

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

000000000046}\proxystubclsid32

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

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

00c04fd7d062}\inprochandler32

HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler32 Opens key:

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

00c04fd7d062}\inprochandlerx86

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

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

00c04fd7d062}\localserver

HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver Opens key: HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-Opens key 00c04f79abd1}\proxystubclsid32

Opens key: $HKCR \verb|\interface| \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\} \verb|\proxystubclsid32|$ $\label{thm:local_hammon_hammon} \textbf{HKLM} \\ \textbf{software} \\ \textbf{microsoft} \\ \textbf{windows nt} \\ \textbf{currentversion} \\ \textbf{image file execution} \\$ Opens key

options\flashplayer18_a_install.exe\rpcthreadpoolthrottle HKCU\software\microsoft\internet explorer\main Opens key:

HKLM\software\microsoft\internet explorer\main Opens key: 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 HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-Opens key

08002b30309d}\inprocserverx86

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

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

08002b30309d}\localserver32

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

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

08002b30309d}\inprochandler32

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

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

08002b30309d}\inprochandlerx86

Opens key: $HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\nprochandlerx86$

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

08002b30309d}\localserver

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

Opens key HKCU\software\microsoft\internet

```
explorer\main\featurecontrol\feature_iedde_register_protocol
                                     HKLM\software\microsoft\internet
  Opens key:
\verb|explorer| \verb|main| featurecontrol| feature\_iedde\_register\_protocol| \\
  Opens key:
                                     \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
options\normaliz.dll
  Opens key
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
                                     HKLM\software\microsoft\windows\currentversion\internet
  Opens kev:
settings\5.0\cache
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\content
                                     HKLM\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\content
  Opens key:
                                     \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current \+ version \+ internet
settings\5.0\cache\cookies
  Opens key:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
                                     \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
  Opens key
settings\5.0\cache\history
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
  Opens key:
                                     \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings\5.0\cache\extensible cache\domstore
  Opens key
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\extensible cache\iecompat
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\install.exe\rpcthreadpoolthrottle
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\extensible cache\ietld
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\extensible cache\mshist012014033120140407
  Opens key:
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ install. execution \ shell \ compatibility \ applications \ install. \\
  Opens key:
HKLM \label{lem:hklm} In the limit of the 
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\extensible cache\privacie:
  Opens key:
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ in stall. exe \ starcraft
1.03
  Opens key:
                                     HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\retry_headeronly post\_on connection reset| \\
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                                     HKCU\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature bufferbreaking 818408
  Opens kev:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature skip post retry on internetwritefile kb895954
                                     HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:
                                     \label{lem:hklmsoftware policies microsoft windows \current version \ \ internet
settings\5.0\cache
  Opens key:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                                     HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:
                                     {\tt HKCU \ } software \verb|\ microsoft \> \ internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:
                                     HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_use\_cname\_for\_spn\_kb911149
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature use spn for ntlm auth disabled
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature allow long international filenames
                                     HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                                     HKLM\software\microsoft\internet
  Opens key:
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
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key
                                     HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_digest_no_extras_in\_uri| \\
```

```
Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens key:
                                      HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature_passport\_check\_302\_for\_success\_kb949059
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
  Opens key:
                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
  Opens key:
                                       HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
\label{lem:hklm} \verb+KKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens kev:
Opens key:
Opens key:
Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000006
  Opens key:
Opens kev:
HKLM \label{lem:hklm} Which is the minimum of the
  Opens key:
Opens kev:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5
  Opens key:
Opens key:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace\_catalog5 \ catalog\_entries
  Opens key
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003
                                      HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens kev:
  Opens key
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:
                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature return failed connect content kb942615
  Opens key:
                                      HKLM\software\policies\microsoft\internet explorer\browseremulation
  Opens key:
                                       HKCU\software\policies\microsoft\internet explorer\browseremulation
  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}
  Opens key:
                                      HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                      HKCU \setminus software \setminus classes \setminus clsid \setminus \{3050f3bc-98b5-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11cf-bb82-11c
00aa00bdce0b}\treatas
  Opens key:
                                      HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\treatas
                                      HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
  Opens key
00aa00bdce0b}\inprocserver32
                                      HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
  Opens key:
  Opens key:
                                      HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
                                      HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
  Opens key:
  Opens key
                                      HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:
                                      HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver32
  Opens key:
                                      HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
  Opens key:
                                      HKCR \verb|\clsid|{3050f3bc-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprochandler32| \\
  Opens key:
                                      HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82-
00aa00bdce0b}\inprochandlerx86
  Opens key:
                                      HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\nprochandlerx86
                                      HKCU\software\classes\clsid\{3050f3bc-98b5-11cf-bb82
  Opens key:
00aa00bdce0b}\localserver
                                      HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\localserver
  Opens key:
  Opens key:
                                      \label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution
options\msls31.dll
  Opens key:
                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mshtml.dll
```

HKCU\software\microsoft\internet

```
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\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
                          HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
 Opens kev:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature aria support
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
                          {\tt HKLM \backslash software \backslash microsoft \backslash internet}
 Opens kev:
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
explorer\main\featurecontrol\feature_css_show_hide_events
 Opens key
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
 Opens key
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
 Opens key
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature allow expanduri bypass
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature allow expanduri bypass
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_databinding_support
 Opens kev:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enforce_bstr
                          HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enforce_bstr
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_dynamic_object_caching
 Opens key
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
                          HKLM\software\microsoft\internet
 Opens kev:
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\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cleanup_at_fls
                          HKLM\software\microsoft\windows\currentversion\app paths\outlook.exe
 Opens key:
 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:
                          \label{lem:hklm} \verb+Kklm \+ 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
                          HKCU\software\microsoft\internet explorer\safety\privacie
 Opens kev:
                          {\tt HKLM \ } software \verb|\ microsoft \ | \ explorer \verb|\ safety \ | \ privacie
 Opens key:
                          HKLM\software\microsoft\internet explorer\mediatypeclass
 Opens key:
 Opens key:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\accepted documents
                          HKLM\software\microsoft\windows\currentversion\policies\ratings
 Opens key:
                          HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615
 Opens key:
                          HKCU\software\classes\exefile\shell
 Opens key:
                          HKCR\exefile\shell
                          HKLM\software\microsoft\windows\currentversion\app paths\msmpeng.exe
 Opens key
                          HKCU\software\classes\applications\msmpeng.exe
 Opens key:
                          HKCR\applications\msmpeng.exe
 Opens key:
 Opens key:
                          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:
                          HKCR\protocols\handler\c
 Opens key:
                          HKCU\software\microsoft\internet explorer
 Opens key:
                          HKLM\software\microsoft\internet explorer
 Opens key:
                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
```

explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120

```
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
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature restrict res to lmz
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature load shdoclc resources
 Opens key:
                         HKLM\software\microsoft\internet
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
                         HKCU\software\classes\protocols\filter\text/html
 Opens key:
 Opens key
                         HKCR\protocols\filter\text/html
                         HKLM\software\microsoft\windows
 Opens key:
nt\currentversion\appcompatflags\custom\msmpeng.exe
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
                          HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
 Opens key:
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
 Opens key
Opens key: 00aa00686f13}\treatas
                          HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens key
00aa00686f13}\inprocserver32
 Opens kev:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens key
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
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
                          HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens key
00aa00686f13}\inprochandlerx86
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandlerx86
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msmpeng.exe
 Opens key:
                          HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
 Opens key:
                         HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
                         HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
 Opens kev:
0000f87a470c}\treatas
                          HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\treatas
 Opens key:
                         HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature manage script circular refs
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_manage_script_circular_refs
                         HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
 Opens key:
0000f87a470c}\inprocserver32
                         HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\ \ \ in procserver 32
 Opens key:
                         HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
 Opens key
0000f87a470c}\inprocserverx86
 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
                         {\tt HKLM \setminus software \setminus microsoft \setminus internet\ explorer \setminus security \setminus floppy\ access}
 Opens key:
                         HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
detection
 Opens key
                          HKLM\software\microsoft\internet explorer\security\adv addrbar spoof
detection
                          HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserverx86
 Opens key:
                         HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
 Opens key
0000f87a470c}\localserver32
                         HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\localserver32
 Opens key:
                         HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
 Opens key
0000f87a470c}\inprochandler32
 Opens key:
                         HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler32
                         HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
 Opens key:
0000f87a470c}\inprochandlerx86
                         HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandlerx86
 Opens kev:
                         HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd
 Opens key:
0000f87a470c}\localserver
                         HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\localserver
 Opens key:
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mpsvc.dll
 Opens key:
                          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
                          HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
 Opens key:
```

```
Opens key:
                                                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
    Opens key:
                                                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\treatas
    Opens key:
                                                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
    Opens key:
                                                        HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
    Opens key:
                                                        HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
                                                        HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
    Opens kev:
00aa00bdce0b}\inprocserverx86
                                                        HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
    Opens kev:
    Opens key
                                                        HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
    Opens key:
                                                        HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver32
    Opens key
                                                        HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
    Opens key:
                                                        HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\tinprochandler32
                                                         HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
    Opens key:
00aa00bdce0b}\inprochandlerx86
                                                        HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86
    Opens key:
    Opens key:
                                                        HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82
00aa00bdce0b}\localserver
    Opens key:
                                                        HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver
    Opens key:
HKCU \setminus software \setminus irrosoft \setminus ir
006097deacf9}
    Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{5e6ab780-7743-11cf-a12b-
00aa004ae837}
    Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\settings
   Opens key
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
   Opens key:
                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cryptui.dll
   Opens key
                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
    Opens key:
                                                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_document_compatible_mode
    Opens key:
options\shdocvw.dll
    Opens key:
                                                         HKLM\system\currentcontrolset\services\tcpip\linkage
    Opens key:
                                                         HKLM\system\currentcontrolset\services\tcpip\parameters\
    Opens key:
                                                         HKLM\software\microsoft\windows\currentversion\internet settings\zones\3
    Opens key:
                                                         HKLM\software\policies\microsoft\internet explorer\zoom
    Opens key:
                                                         HKCU \setminus software \setminus classes \setminus clsid \setminus \{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6\}
    Opens key:
                                                         HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
    Opens key:
                                                         Opens key:
                                                         Opens key:
                                                         HKCU\software\policies\microsoft\internet explorer\zoom
    Opens key:
                                                         HKCU\software\microsoft\internet explorer\zoom
    Opens kev:
                                                        HKLM\software\microsoft\internet explorer\zoom
    Opens key:
                                                         HKCU\software\microsoft\internet
```

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

explorer\main\featurecontrol\feature_weboc document zoom HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_weboc_document_zoom

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

00aa00686f13}\progid

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

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

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

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

options\msmpeng.exe\rpcthreadpoolthrottle

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

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

Opens key: $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc microsoft\internet explorer\international\sc ripts} \\$ Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ internet explorer\+ international\+ scripts$ Opens key: HKLM\software\policies\microsoft\internet explorer\settings

HKCU\software\microsoft\internet explorer\settings Opens kev: 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 kev: Opens key: HKCU\software\microsoft\internet explorer\pagesetup HKCU\software\microsoft\internet explorer\menuext Opens key: HKCU\software\microsoft\internet explorer\menuext\%s Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\codepage

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

Opens key: HKLM\system\currentcontrolset\services\devicesync

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: ${\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus travellog}$ Opens key: HKLM\software\microsoft\internet explorer\version vector

Opens key: HKCU\software\microsoft\internet 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

HKLM\software\microsoft\internet Opens key:

```
explorer\main\featurecontrol\feature_sslux
      Opens key:
                                                                                          HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_browser_emulation| \\
     Opens key:
                                                                                          HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_browser_emulation
                                                                                          HKLM\software\microsoft\windows\currentversion\internet settings\zones\0
      Opens kev:
                                                                                          HKCU\software\microsoft\internet
     Opens key
explorer\main\featurecontrol\feature_xssfilter
     Opens key:
                                                                                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature xssfilter
      Opens key:
                                                                                          HKCU\software\microsoft\windows\currentversion\internet settings\zones
      Opens key:
                                                                                           HKCU\software\classes\msxml2.domdocument.3.0
      Opens key:
                                                                                           HKCR\msxml2.domdocument.3.0
      Opens key:
                                                                                           HKCU\software\classes\msxml2.domdocument.3.0\clsid
      Opens key:
                                                                                           HKCR\mbox{$\backslash$msxml2.domdocument.3.0$} \label{eq:hkcr} Like the constant of t
      Opens key:
                                                                                           HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}
                                                                                           HKCR \ clsid \ \{f5078f32-c551-11d3-89b9-0000f81fe221\}
      Opens key:
      Opens key:
                                                                                           HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\treatas
      Opens key:
                                                                                           HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\treatas
                                                                                          HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
       Opens key:
0000f81fe221}\inprocserver32
      Opens key:
                                                                                          HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32
      Opens key:
                                                                                          HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\inprocserverx86
      Opens key:
                                                                                          HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserverx86
      Opens key:
                                                                                          HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\localserver32
                                                                                          HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\localserver32
      Opens key:
                                                                                          HKCU \setminus software \setminus classes \setminus clsid \setminus \{f5078f32 - c551 - 11d3 - 89b9 - c18f4 -
      Opens key
0000f81fe221}\inprochandler32
                                                                                          HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\ \ in prochandler 32
     Opens key:
      Opens key
                                                                                          HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\inprochandlerx86
                                                                                          HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprochandlerx86
      Opens kev:
                                                                                          HKCU\software\classes\clsid\{f5078f32-c551-11d3-89b9-
      Opens key:
0000f81fe221}\localserver
      Opens key:
                                                                                          HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\localserver
                                                                                           HKU\.default\software\policies\microsoft\control panel\desktop
      Opens kev:
                                                                                           HKU\.default\control panel\desktop
      Opens key:
                                                                                           \label{thm:hkuldefault} \begin{tabular}{ll} HKU\label{thm:hkuldefault} Advanced \end{tabular} Advanced \end{tabular}
      Opens key:
      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:
                                                                                          \label{lem:hkuldefault} HKU \verb|\|.default\| software \verb|\| policies \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet | lem to the le
 settings\zonemap\domains\
     Opens key:
                                                                                          HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                                                                                          HKU\.default\software\microsoft\internet
     Opens kev:
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                                                                          HKU\.default\software\microsoft\windows
     Opens key:
nt\currentversion\appcompatflags\layers
                                                                                          HKLM\software\microsoft\windows
     Opens key:
nt\currentversion\appcompatflags\custom\svchost.exe
      Opens key:
                                                                                           HKLM\software\microsoft\windows nt\currentversion\appcompatflags
      Opens key:
                                                                                           HKCU\software\microsoft\windows nt\currentversion\appcompatflags
      Opens key:
                                                                                           HKU\.default\software\microsoft\windows nt\currentversion\appcompatflags
      Opens key:
                                                                                           HKLM\software\microsoft\windows nt\currentversion\image file execution
options\svchost.exe
      Opens key:
                                                                                           \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
options\acgenral.dll
      Opens key:
                                                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.dll
     Opens key:
                                                                                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\msacm32.dll
     Opens key:
                                                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
      Opens key:
                                                                                           HKLM\software\microsoft\audiocompressionmanager\drivercache
      Opens key
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm
     Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
     Opens key:
                                                                                          HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
      Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610
     Opens key:
                                                                                          HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
      Opens key:
                                                                                          HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
      Opens key:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msaudio 1 \cap msacm \cap 
      Opens key:
\label{thm:hklm} \begin{tabular}{ll} HKLM \end{tabular} is software 
                                                                                           HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.iac2
      Opens key:
      Opens key:
                                                                                           HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. 13 acm
      Opens key:
                                                                                           HKLM\system\currentcontrolset\control\mediaresources\acm
      Opens key:
                                                                                           HKLM\system\currentcontrolset\control\productoptions
      Opens key:
                                                                                           HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| explorer \verb|\| user | leads to be a constant of the constant o
 shell folders
```

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

HKLM\software\policies\microsoft\windows\system

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msxml3.dll Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \directory \shellex \copy hook handlers \end{tabular}$ Opens key: HKCR\directory\shellex\copyhookhandlers Opens key: HKCU\software\classes\directory\shellex\copyhookhandlers\cdf HKCR\directory\shellex\copyhookhandlers\cdf Opens kev: HKLM\software\microsoft\msxm130 Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-Opens kev: 00c04fd75d13}\inprocserver32 HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32 Opens kev: Opens key HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13} Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13} HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-Opens key 00c04fd75d13}\treatas Opens key: $\label{locality} $$ HKCR\clsid{67ea19a0-ccef-11d0-8024-00c04fd75d13}\treat as $$ 136.69 \times 10^{-2}$ and $$ 136.69 \times 10^{$ Opens key: HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserverx86 HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserverx86 Opens kev: Opens key HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\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}\inprochandler32 Opens key HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprochandlerx86 Opens key: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprochandlerx86 Opens key HKCU\software\classes\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\localserver HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\localserver Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{67ea19a0-ccef-11d0-8024-00c04fd75d13} Opens kev: HKCU\software\classes\directorv\shellex\copvhookhandlers\filesvstem HKCR\directory\shellex\copyhookhandlers\filesystem Opens kev: HKCU\software\classes\clsid\{217fc9c0-3aea-1069-a2db-Opens key 08002b30309d}\inprocserver32 Opens key: $HKCR \c1sid \end{217} fc9c0-3aea-1069-a2db-08002b30309d \end{300} in procserver 32$ Opens key HKCU\software\classes\directory\shellex\copyhookhandlers\mydocuments HKCR\directory\shellex\copyhookhandlers\mydocuments Opens key Opens key HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32 Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32 Opens key HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367} Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367} Opens key HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\treatas Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\treatas Opens key HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserverx86 HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserverx86 Opens key: Opens key HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\localserver32 HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\localserver32 Opens kev: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-Opens key 006008059367}\inprochandler32 HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprochandler32 Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-Opens key 006008059367}\inprochandlerx86 Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprochandlerx86 Opens key: HKCU\software\classes\clsid\{ecf03a33-103d-11d2-854d-006008059367}\localserver Opens key: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\localserver Opens key HKLM\software\microsoft\windows nt\currentversion\image file execution options\mydocs.dll Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{ecf03a33-103d-11d2-854d-006008059367} Opens key: $\label{lex-copy-hook-handlers-sharing} HKCU \ software \ classes \ directory \ shellex \ copy-hook \ handlers \ sharing$ Opens key: Opens key: 00aa003ca9f6}\inprocserver32 Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32 $\label{local-bound} HKCU \software \classes \clsid \ \{40dd6e20-7c17-11ce-a804-00aa003ca9f6\}$ Opens key HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6} Opens key: HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-Opens key: 00aa003ca9f6}\treatas Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\treatas HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-Opens key: 00aa003ca9f6}\inprocserverx86 Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserverx86 HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-Opens key 00aa003ca9f6}\localserver32 Opens kev: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\localserver32 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}\localserver Opens key: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\localserver

00aa003ca9f6}\inprochandlerx86

Opens key:

Opens key

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

HKCU\software\classes\clsid\{40dd6e20-7c17-11ce-a804-

```
options\atl.dll
```

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

folders

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

options\ntshrui.dll

Opens kev:

 $HKLM \label{loop} \mbox{HKLM} software \mbox{\sc urrentversion} \label{loop} \mbox{\sc urrentversion} \label{loop} \mbox{\sc urrentversion} \label{loop} \mbox{\sc urrentversion} \label{loop} \mbox{\sc urrentversion} \mbox{\sc urrentversion} \label{loop} \mbox{\sc urrentversion} \mbox{\sc urren$

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

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

explorer\infodelivery\restrictions HKCU\software\policies\microsoft\internet Opens key

explorer\infodelivery\restrictions

Opens key:

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

settings\

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

settings\zonemap\

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

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

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

f4ceaaf59cfc}\inprocserver32

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

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

f4ceaaf59cfc}\inprocserverx86

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

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

f4ceaaf59cfc}\localserver32

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

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

f4ceaaf59cfc}\inprochandler32

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

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

f4ceaaf59cfc}\inprochandlerx86

 $HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\ \ \ in prochandler x 86$ Opens key:

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

f4ceaaf59cfc}\localserver

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

Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution$ options\msimtf.dll

Opens key:

HKLM\software\microsoft\ctf\tip

HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-Opens key: c9633f71be64}\languageprofile

Opens kev:

HKCU\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8c9633f71be64}\languageprofile

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

c9633f71be64}\languageprofile\0x00000000 Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-

c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}

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

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

431b3828ba53}\treatas

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

431b3828ba53}\inprocserver32

 $HKCR \c1sid \ \{3ce74de4-53d3-4d74-8b83-431b3828ba53\} \ \ inprocserver 32$ Opens key:

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

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:

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

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

431b3828ba53}\inprochandlerx86

Opens key:

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

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

431b3828ba53}\localserver

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

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

869523e2d6c7}\treatas

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

869523e2d6c7}\inprocserver32

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

Opens key

869523e2d6c7}\inprocserverx86

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

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

```
869523e2d6c7}\localserver32
                                                                                                               HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver32
       Opens key:
       Opens key
                                                                                                              HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprochandler32
                                                                                                              HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandler32
       Opens key:
                                                                                                               HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
       Opens key
869523e2d6c7}\inprochandlerx86
                                                                                                              HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprochandlerx86
       Opens kev:
                                                                                                              HKCU\software\classes\clsid\{a4b544a1-438d-4b41-9325-
       Opens key
869523e2d6c7}\localserver
       Opens key:
                                                                                                              HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\localserver
       Opens key:
                                                                                                               HKLM\software\microsoft\ctf\tip\
                                                                                                               HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
       Opens key
c9633f71be64}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
       Opens key:
                                                                                                              HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80\} \land category \land \{b95f181b-ea4c-4af1-8056-7c321abbb091\}
      Opens key:
                                                                                                              e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                               HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
       Opens key
00c04fc324a1
                                                                                                  \category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                                                               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 key:
0 f816 c09 f4 ee \} \\ category \\ \{b95 f181 b-ea4 c-4 af1-8056-7 c321 abb b091\}
       Opens key:
                                                                                                               HKCU\software\microsoft\ctf\langbaraddin\
       Opens key:
                                                                                                               {\it HKLM} \ software \ microsoft \ ctf \ language and din \ \ the constraint \ description \ descri
       Opens key
                                                                                                               HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64\\ \\ \\ category\\ \\ \\ \\ \\ 534c48c1-0607-4098-a521-4fc899c73e90\\ \\ \\ \\
                                                                                                               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
       Opens key
                                                                                                      category\{534c48c1-0607-4098-a521-4fc899c73e90}
77e8f3d1aa80}\categor
       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-b3b
                                                                                                   \category\{534c48c1-0607-4098-a521-4fc899c73e90}
e988c088ec82}\categor
                                                                                                              HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
      Opens key
                                                                                                      category\{534c48c1-0607-4098-a521-4fc899c73e90}
00c04fc324a1
                                                                                                               HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
       Opens key
Of816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                                                              HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
      Opens key
c9633f71be64}
                                                                                                  \item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
       Opens key:
                                                                                                               HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                                                               HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
       Opens key:
c9633f71be64}\category
                                                                                                            tem\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
       Opens key
                                                                                                               HKLM \setminus software \setminus microsoft \setminus ctf \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-85
77e8f3d1aa80}\category
                                                                                                   \item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
       Opens key
                                                                                                               HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 80
c9633f71be64}\categor
                                                                                                             tem\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
                                                                                                               HKLM \setminus software \setminus microsoft \setminus ctf \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-85
       Opens key
Opens key
                                                                                                               HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
      Opens key
                                                                                                              77e8f3d1aa80}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
      Opens key
                                                                                                              HKLM\software\microsoft\ctf\tip\{c1ee01f2-b3b6-4a6a-9ddd-
e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
      Opens kev:
                                                                                                              HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
00c04fc324a1}\categorv\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
                                                                                                              HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
       Opens key
Of816c09f4ee}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}
       Opens key:
                                                                                                               HKCU\software\policies\microsoft\internet explorer\control panel
       Opens key:
                                                                                                               HKCU\software\microsoft\windows\currentversion\internet settings\url
history
       Opens key:
                                                                                                               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
       Opens key
                                                                                                               HKLM\software\microsoft\internet
explorer\main
                                                                                                            trol\feature_iedde_register_urlecho
                                                                                                               HKCU\software\microsoft\internet
       Opens key
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 \verb|\clsid| \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\}
       Opens key:
                                                                                                               HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
                                                                                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\treatas
       Opens kev:
                                                                                                              HKCU \setminus software \setminus classes \setminus clsid \setminus \{f414c260-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac0-11cf-b6d1-6ac
       Opens key:
00aa00bbbb58}\inprocserver32
                                                                                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32
       Opens key:
                                                                                                              HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
       Opens key:
00aa00bbbb58}\inprocserverx86
                                                                                                              HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserverx86
       Opens key:
                                                                                                               HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
       Opens key
00aa00bbbb58}\localserver32
       Opens key:
                                                                                                              HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32
                                                                                                              HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
       Opens key
00aa00bbbb58}\inprochandler32
                                                                                                              HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprochandler 32
       Opens kev:
                                                                                                               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
       Opens key:
                                                                                                               HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\localserver
       Opens key
                                                                                                               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jscript.dll
```

HKLM\software\microsoft\windows script\features

HKCU\software\microsoft\internet

Opens key:

```
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
  Opens key:
                                    HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_respect\_objects a fety\_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\svstem\currentcontrolset\control\nls\locale
  Opens kev:
                                    HKLM\svstem\currentcontrolset\control\nls\locale\alternate sorts
                                    HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:
  Opens kev:
                                    HKCU\software\classes\appid\flashplayer18 a install.exe
  Opens key:
                                    HKCR\appid\flashplayer18_a_install.exe
  Opens key:
                                    HKLM\system\currentcontrolset\control\lsa
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_shim_mshelp_combine
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_shim_mshelp_combine
  Opens key:
                                    HKCU \setminus software \setminus classes \setminus clsid \setminus \{81397204 - f51a - 4571 - 8d7b - dc030521aabd\}
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}
  Opens key
  Opens key:
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\treatas
  Opens key:
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\treatas
  Opens key
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprocserver32
  Opens key:
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32
  Opens key
                                    HKCU \setminus software \setminus classes \setminus clsid \setminus \{81397204 - f51a - 4571 - 8d7b - f51a - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6471 - 6
dc030521aabd}\inprocserverx86
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserverx86
  Opens key:
  Opens key
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\localserver32
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\localserver32
  Opens key:
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
  Opens key
dc030521aabd}\inprochandler32
  Opens kev:
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandler32
  Opens key
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\inprochandlerx86
  Opens key:
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprochandlerx86
  Opens key:
                                    HKCU\software\classes\clsid\{81397204-f51a-4571-8d7b-
dc030521aabd}\localserver
  Opens kev:
                                    HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\localserver
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\dxtrans.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
  Opens key:
                                    HKCU \setminus software \setminus classes \setminus clsid \setminus \{d1fe6762 - fc48 - 11d0 - 883a - 3c8b00c10000\}
  Opens key
                                    HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}
  Opens key:
                                    HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\treatas
  Opens key:
                                    HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\treatas
  Opens key
                                    HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserver32
                                    HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32
  Opens key:
  Opens key
                                    HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprocserverx86
                                    HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserverx86
  Opens kev:
                                    HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
  Opens key
3c8b00c10000}\localserver32
                                    HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\localserver32
  Opens key:
                                    HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
  Opens key
3c8b00c10000}\inprochandler32
  Opens key:
                                    HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandler32
  Opens key
                                    HKCU\software\classes\clsid\{d1fe6762-fc48-11d0-883a-
3c8b00c10000}\inprochandlerx86
                                    HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprochandlerx86
  Opens key:
                                    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 key:
  Opens key
                                    HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\treatas
  Opens key:
                                    HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\treatas
                                    HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
  Opens key
00c04fd9189d}\inprocserver32
                                    HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\svchost.exe\rpcthreadpoolthrottle
                                   HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
  Opens key:
00c04fd9189d}\inprocserverx86
                                    HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\
  Opens kev:
                                    HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca
  Opens key:
00c04fd9189d}\localserver32
                                    HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\localserver32
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandler32
  Opens key:
                                    \label{lem:hklmsoftware} \verb+wicrosoft+ windows nt+ current version+ image file execution
options\winsta.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wtsapi32.dll
                                    HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandler32
  Opens key:
```

```
Opens key:
                                             HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprochandlerx86
   Opens key:
                                             HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprochandlerx86
   Opens key:
                                             HKCU\software\classes\clsid\{4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\localserver
                                             HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\localserver
   Opens kev:
   Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc3
   Opens key:
                                              HKLM\software\microsoft\rpc\securityservice
   Opens key:
                                              HKLM\system\currentcontrolset\control\securityproviders
   Opens key:
                                              HKLM\system\currentcontrolset\control\lsa\sspicache
   Opens key:
                                              HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
   Opens key:
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
   Opens key:
                                              HKLM \ system \ current controls et \ control \ lsa \ spicache \ digest. 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:
                                              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:
                                              HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
   Opens key
                                              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
   Opens key:
                                              {\tt HKLM \ } system \verb|\ current control \ } security providers \verb|\ sasl profiles \ |
   Opens key:
                                              \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\msv1_0.dll
   Opens key:
                                              HKLM\system\currentcontrolset\control\session manager\environment
                                              HKU\s-1-5-21-1757981266-507921405-1957994488-1003
   Opens key:
                                              HKU\s-1-5-21-1757981266-507921405-1957994488-1003\environment
   Opens key:
                                              HKU\s-1-5-21-1757981266-507921405-1957994488-1003\volatile environment
   Opens key:
                                              HKU\s-1-5-21-1757981266-507921405-1957994488-
   Opens key:
1003\software\microsoft\windows nt\currentversion\appcompatflags\layers
   Opens kev:
                                             HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\dllhost.exe
                                             HKU\s-1-5-21-1757981266-507921405-1957994488-
   Opens kev:
1003\software\policies\microsoft\control panel\desktop
                                             HKU\s-1-5-21-1757981266-507921405-1957994488-1003\control panel\desktop
   Opens key:
   Opens key:
                                             HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows nt\currentversion\appcompatflags
                                             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
   Opens kev:
                                              HKLM\software\microsoft\directdraw\compatibility\msgolf98
   Opens key:
                                              HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay
   Opens key:
                                              HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo
                                              {\tt HKLM} \\ {\tt software} \\ {\tt microsoft} \\ {\tt directdraw} \\ {\tt compatibility} \\ {\tt rogue} \\ \\ {\tt squadron} \\
   Opens kev:
                                              HKLM\software\microsoft\directdraw\compatibility\savage
   Opens kev:
   Opens key:
                                              HKLM\software\microsoft\directdraw\compatibility\scorchedplanet
                                              HKLM\software\microsoft\directdraw\compatibility\silentthunder
   Opens key:
                                              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:
                                             HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
                                             HKU\s-1-5-21-1757981266-507921405-1957994488-
   Opens key:
1003 \verb|\software\policies\microsoft\windows\safer\code identifiers \verb|\ode| hashes
   Opens key:
                                             HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
                                             HKU\s-1-5-21-1757981266-507921405-1957994488-
   Opens kev:
1003\software\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\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
                                             HKU\s-1-5-21-1757981266-507921405-1957994488-
   Opens key:
1003\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
   Opens key:
                                             HKU\s-1-5-21-1757981266-507921405-1957994488-
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 kev:
                                             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\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
   Opens key:
                                             HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
                                             HKU\s-1-5-21-1757981266-507921405-1957994488-
   Opens key:
1003\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
```

HKLM\software\microsoft\direct3d

```
Opens key:
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:
                                  HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\explorer\shell folders
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options\dllhost.exe
                                   HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
  Opens key:
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}
  Opens key:
  Opens key
                                   HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\treatas
  Opens key:
                                   HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\treatas
  Opens key
                                  HKCU\software\classes\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:
  Opens key
                                  HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231
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:
                                   Opens key:
                                  HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprochandlerx86
                                  Opens key:
  Opens key:
                                  HKCU\software\classes\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\localserver
                                  HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\localserver
  Opens key:
                                   HKLM\software\policies\microsoft\internet explorer\dxtrans
  Opens key:
  Opens kev:
                                   HKCU\software\microsoft\internet explorer\dxtrans
  Opens kev:
                                  HKLM\software\microsoft\internet explorer\dxtrans
                                   HKCU\software\classes\dximagetransform.microsoft.gradient
  Opens kev:
  Opens key:
                                  HKCR\dximagetransform.microsoft.gradient
  Opens key:
                                   HKCU\software\classes\dximagetransform.microsoft.gradient\clsid
  Opens key:
                                   HKCR\dximagetransform.microsoft.gradient\clsid
  Opens key
                                   HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}
                                   HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}
  Opens key
  Opens key:
                                   HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-
0000f8756a10}\treatas
  Opens key
                                   HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\treatas
  Opens key
                                   HKLM\software\microsoft\internet explorer\activex
compatibility\{623e2882-fc0e-11d1-9a77-0000f8756a10}
  Opens key:
                                  HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-
0000f8756a10}\inprocserver32
  Opens key:
                                  HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32
  Opens key:
                                  HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77-
0000f8756a10}\inprocserverx86
                                  HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserverx86
  Opens key:
  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}\inprochandler32
  Opens key:
                                  HKCU\software\classes\clsid\{623e2882-fc0e-11d1-9a77
  Opens key:
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:
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key
options\dllhost.exe\rpcthreadpoolthrottle
  Opens key:
                                   \label{lem:hklm} \verb+ HKLM \+ software \+ icrosoft \+ ctf \+ compatibility \+ dl \+ host. exe
  Opens key:
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dxtmsft.dll
  Opens key:
                                   HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet settings | leaves the setting of the
  Opens key
                                   HKU\.default\software\policies
  Opens key:
                                   HKU\.default\software
                                  HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}
  Opens kev:
                                   HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}
  Opens key:
                                   HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-
  Opens key
00c04fd9189d}\treatas
                                   HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\treatas
  Opens key:
                                  HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-
  Opens key
00c04fd9189d}\inprocserver32
                                  HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\ inprocserver32
  Opens key:
  Opens key:
                                  HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-
00c04fd9189d}\inprocserverx86
                                  \label{local-condition} HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\\\ \label{local-condition} \label{local-condition}
  Opens key:
  Opens key:
                                  HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-
00c04fd9189d}\localserver32
                                  HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\localserver32
  Opens key:
  Opens key:
                                  HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:
                                  HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-
00c04fd9189d}\inprochandler32
  Opens key:
                                  \label{local-condition} HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\\\ \inprochandler 32
  Opens key
                                   HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-
00c04fd9189d}\inprochandlerx86
                                  HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprochandlerx86
  Opens key:
```

HKCU\software\classes\clsid\{c6365470-f667-11d1-9067-

```
00c04fd9189d}\localserver
 Opens key:
                        HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
 Opens key:
                        HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\localserver
                        HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
 Opens key:
                        HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}
 Opens kev:
 Opens kev:
                        HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\treatas
                        HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\treatas
 Opens key:
 Opens key
                        HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32
 Opens key:
                        HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32
                        HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
 Opens key
0000f87557db}\inprocserverx86
                        Opens key:
 Opens key:
                        HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e
0000f87557db}\localserver32
                        HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\localserver32
 Opens key:
                        HKU\.default\software\microsoft\windows\currentversion\internet
 Opens key
settings\5.0\cache\cookies
                        HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
 Opens key:
0000f87557db}\inprochandler32
 Opens key:
                        HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprochandler32
 Opens key:
                        HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprochandlerx86
 Opens key:
                        Opens key:
                        HKCU\software\classes\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\localserver
                        HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\localserver
 Opens key:
                        HKU\.default\software\microsoft\windows\currentversion\internet
 Opens key
settings\5.0\cache\history
                        Opens key:
settings\5.0\cache\extensible cache
                        HKU\.default\software\microsoft\windows\currentversion\internet
 Opens key
settings\5.0\cache\extensible cache\ietld
                        HKU\.default\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\cache\extensible cache\mshist012013122320131224
 Opens key:
                        \label{locality} HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\}
 Opens key
                        HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}
                        HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
 Opens key
f4fc1e6ca1bd}\treatas
                        HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\treatas
 Opens key
 Opens key
                        HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32
                        HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\ \ inprocserver 32
 Opens key
 Opens key
                        HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserverx86
 Opens key:
                        HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserverx86
 Opens key
                        HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\localserver32
                        HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\localserver32
 Opens key
 Opens key:
                        HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprochandler32
                        HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandler32
 Opens kev:
                        HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
 Opens key
f4fc1e6ca1bd}\inprochandlerx86
 Opens key:
                        HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprochandlerx86
                        HKCU\software\classes\clsid\{385a91bc-1e8a-4e4a-a7a6-
 Opens key:
f4fc1e6ca1bd}\localserver
 Opens key:
                        HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\localserver
 Opens key:
                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sxs.dll
 Opens key:
                        HKCU\software\classes\typelib
 Opens key:
                        HKCR\typelib
 Opens key:
                        HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
 Opens key:
                        HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}
 Opens key:
                        HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
 Opens key:
                        HKCR\tvpelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1
 Opens key:
                        00aa003b6061}\1.1\409
 Opens key:
                        HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\409
                        HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
 Opens key
00aa003b6061}\1.1\9
                        HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\9
 Opens key:
Opens key:
00aa003b6061}\1.1\0
                        HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
                        HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0
 Opens key:
                        HKCU\software\classes\typelib\{5e77eb03-937c-11d1-b047-
 Opens key
00aa003b6061}\1.1\0\win32
 Opens key:
                        HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32
 Opens key:
                        HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                        HKU\.default\software\microsoft\windows\currentversion\internet
 Opens key:
settings\wpad
 Opens key:
                        HKU\.default\software\microsoft\windows\currentversion\internet
settings\http filters\rpa
                        HKLM\software\microsoft\windows\currentversion\internet settings\http
 Opens key:
filters\rpa
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
 Opens key:
                        HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
 Opens key:
                        HKCR\typelib\{00020430-0000-0000-c000-00000000046}
 Opens key:
                        HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}\2.0
```

HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0

```
Opens key:
                                    HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0
                                    HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0
  Opens key:
  Opens key:
                                    \label{thm:local_equation} \begin{tabular}{ll} HKCU \software \classes \typelib \classes \c
000000000046}\2.0\0\win32
                                    HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32
  Opens kev:
  Opens kev:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasman.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rtutils.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
  Opens key:
                                    HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
                                    HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}
  Opens key:
                                    HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
  Opens key:
  Opens key:
                                    HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1
                                    HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
  Opens key:
0000f87557db}\1.1\409
                                    HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\409
  Opens key
  Opens key:
                                    HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1
0000f87557db}\1.1\9
  Opens key:
                                    HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\9
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\telephony
  Opens key:
                                    \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\rasapi32.dll
  Opens key:
                                    HKLM\software\microsoft\tracing\rasapi32
                                    Opens key:
0000f87557db}\1.1\0
                                    HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0
  Opens key:
                                    HKCU\software\classes\typelib\{54314d1d-35fe-11d1-81a1-
  Opens key
0000f87557db}\1.1\0\win32
                                    HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32
  Opens key:
  Opens key
                                    HKCU\software\microsoft\internet
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\opera software
  Opens key:
                                    HKCU\software\microsoft\ftp
  Opens key
                                    HKLM\software\policies\microsoft\internet explorer\services
  Opens key:
                                    HKCU\software\microsoft\internet explorer\services
                                    HKLM\software\microsoft\internet explorer\services
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\activities
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet explorer\activities
  Opens key:
                                    HKLM\software\microsoft\internet explorer\activities
  Opens key:
                                    HKLM\software\policies\microsoft\internet explorer\suggested sites
  Opens key:
                                    \label{lem:hkcu} \mbox{HKCU\software\mbox{\tt microsoft\internet explorer\suggested sites}} \\
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sensapi.dll
                                    \label{local-bound} HKCU \software \classes \clsid \ \{0e890f83-5f79-11d1-9043-00c04fd9189d\} \\
  Opens key:
  Opens key:
                                    HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}
                                    HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
  Opens key
00c04fd9189d}\treatas
  Opens key:
                                    HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\treatas
                                    HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
  Opens key
00c04fd9189d}\inprocserver32
                                    HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32
  Opens key:
                                    HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
  Opens key
00c04fd9189d}\inprocserverx86
  Opens key:
                                    HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserverx86
  Opens key
                                    HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\localserver32
  Opens key:
                                    HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\localserver 32
                                    HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
  Opens key:
00c04fd9189d}\inprochandler32
  Opens key:
                                    HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprochandler 32
  Opens key:
                                    HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\inprochandlerx86
  Opens key:
                                    Opens key:
                                    HKCU\software\classes\clsid\{0e890f83-5f79-11d1-9043-
00c04fd9189d}\localserver
  Opens key:
                                    HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\localserver
  Opens kev:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.dll
Opens key: options\dnsapi.dll
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
                                    HKLM\system\currentcontrolset\services\dnscache\parameters
                                    HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:
  Opens key
                                    \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} icrosoft \end{tabular} icrosoft \end{tabular} icrosoft \end{tabular} icrosoft \end{tabular} strong
cryptographic provider
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
  Opens key:
                                    HKLM\software\policies\microsoft\cryptography
  Opens key:
                                    HKLM\software\microsoft\cryptography
                                    HKLM\software\microsoft\cryptography\offload
  Opens key
  Opens key:
                                    HKCU\software\microsoft\internet
explorer \verb|`main| featurecontrol| feature\_activex\_inactivate\_mode\_removal\_revert
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_subdownload_lockdown
  Opens key:
                                    HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_subdownload\_lockdown| \\
  Opens key:
                                    HKCU\software\microsoft\internet
```

 $\verb|explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation| \\$

```
Opens key:
                                                                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation
     Opens key:
                                                                                        HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_block_lmz_script| \\
     Opens key:
                                                                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature block lmz script
     Opens key:
                                                                                        HKCU\software\microsoft\windows\currentversion\internet settings\user
agent
                                                                                         HKLM\software\microsoft\windows\currentversion\internet settings\user
     Opens key:
agent
     Opens key:
                                                                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
     Opens key
                                                                                         HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
     Opens key:
                                                                                         HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\ua tokens
     Opens key:
                                                                                         HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\pre platform
      Opens key:
                                                                                         HKLM\software\microsoft\windows\currentversion\internet
 settings\5.0\user agent\pre platform
                                                                                         HKCU\software\microsoft\windows\currentversion\internet
      Opens key:
settings\5.0\user agent\pre platform
     Opens key:
                                                                                        HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\post platform
      Opens key:
                                                                                         HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
     Opens key
                                                                                         HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\user agent\post platform
                                                                                         HKCU\software\classes\http\shell\open\command
      Opens key:
                                                                                        HKCR\http\shell\open\command
      Opens key:
     Opens key:
                                                                                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature scripturl mitigation
      Opens kev:
                                                                                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature scripturl mitigation
                                                                                        HKLM\software\microsoft\windows\currentversion\internet settings\winhttp
      Opens kev:
     Opens key:
                                                                                        HKLM\software\microsoft\windows\currentversion\internet
settings\connections
     Opens key:
                                                                                         HKLM\software\microsoft\windows\currentversion\internet
 settings\winhttp\unsafesslapps
                                                                                         HKCU\software\microsoft\windows\currentversion\internet
      Opens key:
settings\connections
      Opens key:
                                                                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\schannel.dll
      Opens key:
                                                                                         HKCU\software\microsoft\cryptography\providers\type 012
      Opens key
                                                                                         HKLM\software\microsoft\cryptography\defaults\provider types\type 012
      Opens key:
                                                                                         HKLM \label{lem:hcm} \label{lem:hcm} HKLM \label{lem:hcm} In the lem \label{lem:hcm} HKLM \label{lem:hcm} \label{lem:hcm} HKLM \label{lem:hcm} \label{lem:hcm} \label{lem:hcm} HKLM \label{lem:hcm} \label{lcm} \labell} \label{lcm} \label{lcm} \labell{lcm} \labell} \labell{lcm} \labell{lcm} \labell} \labell{lcm} \labell{lcm} \labell{lcm} \labell} \labell{lcm} \labell{lcm} \labell{lcm} \labell} \labell{lc
 schannel cryptographic provider
      Opens key:
                                                                                         {\tt HKLM} \verb|\software\microsoft\cryptography\deshashsessionkeybackward\\
     Opens key
                                                                                        Opens key:
                                                                                         HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ types \ \ type \ \ 018
                                                                                        \label{lem:hklm} \mbox{HKLM\software\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{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{
     Opens key:
schannel cryptographic provider
     Opens kev:
                                                                                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dssenh.dll
     Opens key:
                                                                                         HKLM\software\microsoft\crvptographv\oid
      Opens key:
                                                                                         HKLM\software\microsoft\cryptography\oid\encodingtype 0
                                                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
     Opens key:
0\certdllopenstoreprov
     Opens key:
                                                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\#16
      Opens key:
                                                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\ldap
      Opens key:
                                                                                         HKLM\software\microsoft\cryptography\oid\encodingtype 1
                                                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
      Opens key
 1\certdllopenstoreprov
      Opens key:
                                                                                         HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdlldecodeobjectex
      Opens key
                                                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
 1\cryptdlldecodeobjectex
     Opens key
                                                                                        1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.1.1
                                                                                        Opens key
1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.1
     Opens key
                                                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.11
     Opens key
                                                                                        {\tt HKLM \ } software \verb|\ microsoft \ \ cryptography \verb|\ oid \ \ encoding type \ \ \ )
 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.12
                                                                                        {\tt HKLM} \verb|\software\microsoft\cryptography\oid\encodingtype | } \\
     Opens key
 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.2
                                                                                        {\tt HKLM \coftware \microsoft \cryptography \coid \encoding type}
     Opens key
 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.3
                                                                                        HKLM\software\microsoft\cryptography\oid\encodingtype
     Opens key:
 1\cryptdlldecodeobjectex\1.2.840.113549.1.9.16.2.4
      Opens kev:
HKLM \setminus software \setminus irros of t \setminus cryptography \setminus providers \setminus trust \setminus certificate \setminus \{573e31f8-aaba-11d0-8ccb-12d6\} + (573e31f8-aaba-11d0-8ccb-12d6) + (576e31f8-aaba-12d6) + (576e
00c04fc295ee}
      Opens key:
HKLM \ software \ microsoft \ cryptography \ providers \ trust \ final policy \ \{573e31f8-aaba-11d0-8ccb-dryptography\} \ providers \ trust \ final policy \ for the providers \ for the 
00c04fc295ee}
      Opens key:
HKLM \ software \ icrosoft \ cryptography \ providers \ trust \ initialization \ \{573e31f8-aaba-11d0-8ccb-1464-4644, aba-11d0-8ccb-14644, aba-1464-4644, aba-1464-464, ab
00c04fc295ee}
     Opens key:
                                                                                         HKLM \ software \ `microsoft \ cryptography \ providers \ trust \ `message \ \{573e31f8-microsoft \ cryptography \ orders \ trust \ `message \ and \ orders \ orders
```

aaba-11d0-8ccb-00c04fc295ee}

```
Opens key:
HKLM \ software \ microsoft \ cryptography \ providers \ trust \ signature \ \{573e31f8-aaba-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11
00c04fc295ee}
             Opens key:
HKLM \ software \ microsoft \ cryptography \ providers \ trust \ certcheck \ \{573e31f8-aaba-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11
00c04fc295ee}
             Opens kev:
HKLM\software\microsoft\cryptographv\providers\trust\diagnosticpolicv\{573e31f8-aaba-11d0-8ccb-
00c04fc295ee3
                                                                                                                                                                                                           HKLM \ software \ microsoft \ cryptography \ providers \ trust \ cleanup \ \{573e31f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641f8-641
               Opens key
 aaba-11d0-8ccb-00c04fc295ee}
             Opens key:
                                                                                                                                                                                                           HKCU\software\microsoft\cryptography\providers\type 001
               Opens key:
                                                                                                                                                                                                           HKLM\software\microsoft\cryptography\defaults\provider types\type 001
               Opens key:
                                                                                                                                                                                                           HKCU\software\microsoft\internet explorer\security
               Opens key:
 \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} soft \label{
             Opens key:
 \label{thm:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \system certificates \trusted publisher \safer \end{tabular}
                                                                                                                                                                                                           HKLM\software\microsoft\systemcertificates\trustedpublisher\safer
               Opens key:
               Opens key:
                                                                                                                                                                                                           HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllcreatecertificatechainengine\config
               Opens key:
                                                                                                                                                                                                           HKCU \setminus software \setminus microsoft \setminus system certificates \setminus root \setminus physical stores
               Opens key:
                                                                                                                                                                                                           HKLM \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus root \setminus protected roots
             Opens key:
                                                                                                                                                                                                           \label{lem:hkcu} \verb+KCU\+software\+microsoft\+systemcertificates\+root\+protected roots
               Opens key:
                                                                                                                                                                                                           HKCU\software\microsoft\systemcertificates\root\
               Opens key:
                                                                                                                                                                                                           HKLM \setminus software \setminus microsoft \setminus system certificates \setminus root \setminus physical stores
               Opens key:
                                                                                                                                                                                                           HKLM\software\microsoft\systemcertificates\root\
               Opens key:
HKLM \ software \ microsoft \ system certificates \ 18f7c1fcc3090203fd5baa2f861a754976c8dd25
             Opens kev:
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus root \setminus certificates \setminus 245c97df7514e7cf2df8be72ae957b9e04741e85 \setminus root \setminus ro
             Opens key:
HKLM\software\microsoft\svstemcertificates\root\certificates\7f88cd7223f3c813818c994614a89c99fa3b5247
             Opens kev:
Opens key:
HKLM \ software \ microsoft \ system certificates \ 'codd 4ee ae 6000 ac 7f 40 c 3802 c 171 e 3014 8030 c 072 ac 2014 ac 3014 8030 c 171 e 3014 8030 c 171
               Opens kev:
                                                                                                                                                                                                           HKLM\software\microsoft\systemcertificates\authroot\
               Opens kev:
HKLM \label{eq:hklm} KLM \label{eq:hklm} HKLM \label{eq:hklm} Software \label{eq:hklm} with root \label{eq:hklm} With the label{eq:hklm} With the label{eq:hkklm} With the label{eq:hkkl
               Opens key:
 Opens key:
HKLM \label{lem:hklm} Software \verb|\microsoft| system certificates \verb|\authroot| certificates \verb|\authroot| 202faf 3e 291435468607857694 df 5e 45b 68851868 df 5e 45b 6
               Opens key:
Opens key:
HKLM \label{lem:hklm} IN 1056 a fe9fd0f5 be01685 a acce6a5d1c4454 constraints and the constraints and the constraints and the constraints are constraints are constraints and the constraints are constraints are constraints and the constraints are constraints and the constraints are constraints and the constraints are constraints are constraints are constraints and the constraints are constraints are constraints and the constraints are constraints and the co
             Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\0b77bebbcb7aa24705decc0fbd6a02fc7abd9b52
             Opens key:
             Opens key:
             Opens kev:
             Opens key:
             Opens key:
             Opens key:
```

 $HKLM \label{lem:hklm} In the label{lem:hklm} HKLM \label{lem:hklm} In the label{lem:hklm} HKLM \label{lem:hklm} In the label{lem:hklm} In the label{lem:hklm}$

 $HKLM \ software \ microsoft \ system certificates \ authroot \ certificates \ 209900b63d955728140cd13622d8c687a4eb0085$

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} with root \label{lem:hklm} Certificates \label{lem:hklm} \label{lem:hklm} A \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} White \label{lem:hkklm} Whit$ Opens key:

 $HKLM \ software \ microsoft \ system certificates \ \ authroot \ \ certificates \ \ 24ba6d6c8a5b5837a48db5fae919ea675c94d217$ Opens key:

Opens key:

Opens key:

Opens key:

HKLM\software\microsoft\systemcertificates\authroot\certificates\317a2ad07f2b335ef5a1c34e4b57e8b7d8f1fca6 Opens key:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} where \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lklm} With \label{l$ Opens key: $HKLM \ software \ microsoft \ system certificates \ authroot \ certificates \ 394ff6850b06be52e51856cc10e180e882b385cc$

Opens key:

Opens key:

Opens key: $HKLM \setminus software \setminus microsoft \setminus system certificates \setminus authroot \setminus certificates \setminus 40e78c1d523d1cd9954fac1a1ab3bd3cbaa15bfc$

Opens key: $HKLM \setminus software \setminus microsoft \setminus system certificates \setminus authroot \setminus certificates \setminus 43ddb \mid ffff 3b 49b 73831407f6 bc 8b 975023d07c50$ Opens key:

 $HKLM \ software \ `microsoft\ 'system certificates \ '4463c531d7ccc1006794612bb656d3bf8257846f' \ in the contract of the con$

Opens key: $HKLM \label{lem:hklm} Which is the latest and the$

Opens key:

Opens key:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} with root \label{lem:hklm} Software \label{lem:hklm} With root \label{lem:hklm} With \label{lem:hklm} With root \label{lem:hklm} With root \label{lem:hklm} With root \label{lem:hklm} With root \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} Wi$

- HKLM\software\microsoft\systemcertificates\authroot\certificates\4c95a9902abe0777ced18d6accc3372d2748381e Opens key:
- $\label{thm:hklmsoftware} HKLM \software \mbox{\sim hklmsoftware \mb$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\4efced9c6bdd0c985ca3c7d253063c5be6fc620c Opens key: HKLM\software\microsoft\systemcertificates\authroot\certificates\4f65566336db6598581d584a596c87934d5f2ab4
- Opens key:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\58119f0e128287ea50fdd987456f4f78dcfad6d4
 Opens key:
 HKLM\software\microsoft\systemcertificates\authroot\certificates\5b4e0ec28ebd8292a51782241281ad9feedd4e4c
- Opens key:

 HKLM\software\microsoft\svstemcertificates\authroot\certificates\5d989cdb159611365165641b560fdbea2ac23ef1
- Opens key:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\5e5a168867bfff00987d0b1dc2ab466c4264f956
 Opens key:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\5e997ca5945aab75ffd14804a974bf2ae1dfe7e1 Opens key:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25
 Opens key:
- $\label{thm:local-continuous} HKLM \software \microsoft \system certificates \authroot \certificates \627f8d7827656399d27d7f9044c9feb3f33efa9a Opens key:$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\6372c49da9fff051b8b5c7d4e5aae30384024b9c Opens key:
- $\label{thm:local-continuous} HKLM \software \microsoft \system certificates \authroot \certificates \6782aae0e deee 21a5839d3c0cd14680a4f60142aOpens~key:$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\67eb337b684ceb0ec2b0760ab488278cdd9597dd Opens key:
- $\label{thklm} \begin{tabular}{l} HKL\begin{tabular}{l} HKL\begin{tabular}{l} MKL\begin{tabular}{l} MKL\begin{tabular} MKL\begin{tabular}{l} MKL\begin{tabular}{l} MKL\begin{ta$
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} With the lem \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} With the lem \label{lem:hklm} Software \label{lem:hklm} With the lem \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} With the lem \label{lem:hklm} Software \label{lem:hklm} With the lem \label{lem:hklm} Software \label{lem:hklm} With the lem \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} With the lem \label{lem:hklm} Software \label{lem:hklm} With the lem \label{$
- $\label{thm:local-continuous} HKL\@M\Software\@microsoft\systemcertificates\authroot\certificates\69bd8cf49cd300fb592e1793ca556af3ecaa35fb\\ Opens\ key:$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\6a174570a916fbe84453eed3d070a1d8da442829 Opens key:
- $\label{thm:local-continuous} HKLM \software \mbox{\tt microsoft} system certificates \authroot \certificates \authroot \certif$
- $\label{thm:local-continuous} HKLM \software \microsoft \system certificates \authroot \certificates \74207441729 cdd 92 ec 7931 d823108 dc 28192 e 2 bb \\Opens \ key:$
- $\label{thm:local-continuous} HKLM \software \microsoft \system certificates \authroot \certificates \742c3192e607e424eb4549542be1bbc53e6174e2 \ Opens key: \\ HKLM \software \microsoft \system certificates \authroot \certificates \7639c71847e151b5c7ea01c758fbf12aba298f7a$
- $Opens \ key: \\ HKLM \ software \ microsoft \ system certificates \ authroot \ certificates \ 78e9dd0650624db9cb36b50767f209b843be15b3$
- Opens key:

 HKLM\software\microsoft\systemcertificates\authroot\certificates\7a74410fb0cd5c972a364b71bf031d88a6510e9e
- Opens key:

 HKLM\software\microsoft\systemcertificates\authroot\certificates\7ac5fff8dcbc5583176877073bf751735e9bd358

 Opens key:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\7ca04fd8064c1caa32a37aa94375038e8df8ddc0
- Opens key: HKLM\software\microsoft\systemcertificates\authroot\certificates\7e784a101c8265cc2de1f16d47b440cad90a1945 Opens key:
- WKLM\software\microsoft\systemcertificates\authroot\certificates\81968b3aef1cdc70f5fa3269c292a3635bd123d3
 Opens key:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\838e30f77fdd14aa385ed145009c0e2236494faa Opens key:
- WKLM\software\microsoft\systemcertificates\authroot\certificates\85371ca6e550143dce2803471bde3a09e8f8770f Opens key:
- $\label{thm:local-continuous} HKLM \software \microsoft \system certificates \authroot \certificates \85a408c09c193e5d51587dcdd61330fd8cde37bf \ Opens \ key:$
- NKLM\software\microsoft\systemcertificates\authroot\certificates\879f4bee05df98583be360d633e70d3ffe9871af Opens key:
- WKLM\software\microsoft\systemcertificates\authroot\certificates\8eb03fc3cf7bb292866268b751223db5103405cb Opens key:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\9078c5a28f9a4325c2a7c73813cdfe13c20f934e
- Opens key:

 HKLM\software\microsoft\systemcertificates\authroot\certificates\90aea26985ff14804c434952ece9608477af556f

 Opens key:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\90dede9e4c4e9f6fd88617579dd391bc65a68964
 Opens key:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\96974cd6b663a7184526b1d648ad815cf51e801a Opens key:
- $\label{thm:local-cont} HKLM \software \mbox{$\tt MKLM} \software \mbox{$
- $\label{thm:hklmsoftware} HKLM \software \microsoft \system certificates \authroot \certificates \97e2e99636a547554f838fba38b82e74f89a830a \\Opens \ key:$
- $\label{thm:local-base} HKL\dot{M} software \verb|\microsoft| system certificates \authroot \verb|\certificates| 99a69be61afe886b4d2b82007cb854fc317e1539 Opens key:$
- $\label{thm:local-back} HKLM \software \mbox{$\mbox{}\mbox{$\mbox{\mbo
- $\label{thm:local-continuous} HKLM \software \mbox{\tt microsoft} system certificates \authroot \certificates \9e6ceb 179185 a 29ec 6060 c a 53e1974 a f 94af 59d4 \norm{\tt Opens} key:$
- $\label{thm:local-continuous} HKLM \software \mbox{$\tt microsoft} system certificates \authroot \certificates \9fc796e8f8524f863ae1496d381242105f1b78f5 \end{tikzpicture} Opens key:$

HKLM\software\microsoft\systemcertificates\authroot\certificates\a3e31e20b2e46a328520472d0cde9523e7260c6d Opens key:

NKLM\software\microsoft\systemcertificates\authroot\certificates\a5ec73d48c34fcbef1005aeb85843524bbfab727 Opens key:

 $\label{thm:local-continuous} HKLM \software \mbox{$\mbox{$\mathbb{N}$} irros of tsystem certificates \aced 5f6553fd 25ce 015f1f7a 483b 6a749f6178c6} Opens \ key:$

 $\label{thm:local-bound} HKL\begin{tabular}{l} HKL\begin{tabular}{l} HKL\begin{tabular}{l} MKL\begin{tabular}{l} MKL\begin{tabular}$

 $\label{thm:local-continuous} HKLM \software \mbox{\tt microsoft} system certificates \authroot \certificates \b19dd096dcd4e3e0fd676885505a672c438d4e9cOpens key:$

 $\label{thm:local-continuous} HKLM \software \microsoft \system certificates \authroot \certificates \b3eac44776c9c81ceaf29d95b6cca0081b67ec9d \\Opens \key:$

 $\label{thklm} HKLM \software \microsoft \system certificates \authroot \certificates \b5d303bf8682e152919d83f184ed05f1dce5370cOpens~key:$

HKLM\software\microsoft\systemcertificates\authroot\certificates\b6af5be5f878a00114c3d7fef8c775c34ccd17b6
 Opens key:

HKLM\software\microsoft\systemcertificates\authroot\certificates\b72fff92d2ce43de0a8d4c548c503726a81e2b93
Opens key:

HKLM\software\microsoft\systemcertificates\authroot\certificates\bc9219ddc98e14bf1a781f6e280b04c27f902712 Opens key:

 $\label{thm:local-continuous} HKLM \software \microsoft \system certificates \authroot \certificates \be 36a4562fb2ee 05dbb3d32323adf445084ed656\\ Opens key:$

HKLM\software\microsoft\systemcertificates\authroot\certificates\cabb51672400588e6419f1d40878d0403aa20264
Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\cfdefe102fda05bbe4c78d2e4423589005b2571d

Opens key: HKLM\software\microsoft\systemcertificates\authroot\certificates\cff360f524cb20f1fead89006f7f586a285b2d5b

Opens key: HKLM\software\microsoft\systemcertificates\authroot\certificates\cff810fb2c4ffc0156bfe1e1fabcb418c68d31c5

Opens key: HKLM\software\microsoft\systemcertificates\authroot\certificates\d23209ad23d314232174e40d7f9d62139786633a

Opens key: HKLM\software\microsoft\systemcertificates\authroot\certificates\d29f6c98befc6d986521543ee8be56cebc288cf3

Opens key: HKLM\software\microsoft\systemcertificates\authroot\certificates\d2edf88b41b6fe01461d6e2834ec7c8f6c77721e Opens kev:

HKLM\software\microsoft\systemcertificates\authroot\certificates\da40188b9189a3edeeaeda97fe2f9df5b7d18a41
 Opens key:

 $\label{thm:local-condition} HKLM \software \microsoft \system certificates \authroot \certificates \dbac3c7aa4254da1aa5caad68468cb88eeddeea8 \ Opens key: \\ HKLM \software \microsoft \system certificates \authroot \certificates \de28f4a4ffe5b92fa3c503d1a349a7f9962a8212 \dbackets \dbac$

 $Opens~key: \\ HKLM\software\microsoft\systemcertificates\authroot\certificates\e12dfb4b41d7d9c32b30514bac1d81d8385e2d46$

Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\e392512f0acff505dff6de067f7537e165ea574b

Opens key:
HKLM\software\microsoft\systemcertificates\authroot\certificates\e5df743cb601c49b9843dcab8ce86a81109fe48e
Opens kev:

HKLM\software\microsoft\systemcertificates\authroot\certificates\ebbc0e2d020ca69b222c2bffd203cb8bf5a82766

Opens key:

WKLM\software\microsoft\systemcertificates\authroot\certificates\ec0c3716ea9edfadd35dfbd55608e60a05d3cbf3
Opens key:

 $\label{thm:local-condition} HKLM \software \mbox{\tt microsoft} system certificates \authroot \certificates \ef2 daccbeab 682 d32 ce4 abd 6 cb 90025236 c07 bc. Opens key:$

HKLM\software\microsoft\systemcertificates\authroot\certificates\f44095c238ac73fc4f77bf8f98df70f8f091bc52 Opens key:

 $HKLM \setminus software \setminus microsoft \setminus system certificates \setminus authroot \setminus certificates \setminus f88015d3f98479e1da553d24fd42ba3f43886aeffer to the first of the firs$

Opens key: HKLM\software\microsoft\enterprisecertificates\root\physicalstores

Opens key: HKLM\software\microsoft\enterprisecertificates\root\
Opens key: HKCU\software\microsoft\systemcertificates\ca\physicalstores

Opens key: $\label{local-opens} \mbox{ HKCU\software\mbox{\sc microsoft\system} certificates\ca\end{\sc heavy} $$ \mbox{\sc microsoft\system} $$ \mbox{\sc$

Opens key: HKLM\software\microsoft\systemcertificates\ca\physicalstores

Opens key: HKLM\software\microsoft\systemcertificates\ca\

Opens key:

HKLM\software\microsoft\systemcertificates\ca\certificates\063da67748f0eccc690d319bcdcd0e72ac8d48d5
Opens key:

 $\label{thm:loss} HKLM \software \microsoft \system certificates \ca\certificates \allowed 645bb 78b3ea 2b94c0697c740733031cOpens key:$

HKLM\software\microsoft\systemcertificates\ca\certificates\189271e573fed295a8c130eaf357a20c4a9f115e
 Opens key:
HKLM\software\microsoft\systemcertificates\ca\certificates\2d69a20ec4f0cd19037fd6d6246b1ee0ec41ba22

 $Opens~key: \\ HKLM\software\microsoft\systemcertificates\ca\certificates\7b02312bacc59ec388feae12fd277f6a9fb4fac1$

Opens key: HKLM\software\microsoft\systemcertificates\ca\certificates\8b24cd8d8b58c6da72ace097c7b1e3cea4dc3dc6 Opens key:

HKLM\software\microsoft\systemcertificates\ca\certificates\9f025d9f58711a605eb0694b0e8bc0ca4f25fd6f
Opens kev:

HKLM\software\microsoft\systemcertificates\ca\certificates\ba9e3c32562a67128caabd4ab0c500bee1d0c256 Opens key:

 $\label{thm:local} HKLM \software \mbox{\sc microsoft} system certificates \ca\certificates \esc 215d3460c2c20bbe2d9fe5fb665daa2c0e225cOpens~key:$

 $\label{thm:local} HKLM \software \microsoft \system certificates \ca\certificates \f6357239b7c39725bd8000646e4a0d18ebce4cfa\\ Opens \ key:$

 $HKLM \setminus software \setminus microsoft \setminus system certificates \setminus cartificates \setminus fee 449 ee 0 e 3965 a 5246 f 000 e 87f de 2a065 f d 89d4 e 2a065 f d 89d5 e 2a065 f d 89d5$

Opens key:

Opens kev: HKLM\software\microsoft\enterprisecertificates\ca\physicalstores HKLM\software\microsoft\enterprisecertificates\ca\ Opens key:

Opens key: ${\tt HKCU \setminus software \setminus \dot{m} icrosoft \setminus system certificates \setminus disallowed \setminus physical stores}$

HKCU\software\microsoft\systemcertificates\disallowed\ Opens kev:

Opens key: HKLM\software\microsoft\systemcertificates\disallowed\physicalstores

HKLM\software\microsoft\systemcertificates\disallowed\ Opens kev:

Opens key:

 $HKLM \label{lowed} NKLM \label{lowed} HKLM \label{lowed} White \label{lowed} HKLM \label{lowed} HKLM \label{lowed} White \label{lowed} HKLM \label{lowed} White \label{lowed} HKLM \label{lowed} White \label{lowed} White \label{lowed} HKLM \label{lowed} White \label{lowed} HKLM \label{lowed} White \label{lowed} White \label{lowed} HKLM \label{lowed} White \label{lowed} HKLM \label{lowed} White \label{lo$ Opens key:

 $HKL\ M \ Noftware \ Nicrosoft \ No system certificates \ Visible \ No software \ No system \ No syst$

Opens key: ${\tt HKLM} \verb|\software\m| icrosoft\enterprise certificates\disallowed\physical stores | \\$

Opens key: HKLM\software\microsoft\enterprisecertificates\disallowed\ Opens key: HKCU\software\microsoft\systemcertificates\disallowed\certificates

Opens key: HKCU\software\microsoft\systemcertificates\disallowed\crls Opens key: HKCU\software\microsoft\systemcertificates\disallowed\ctls

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

Opens key: HKCU\software\policies\microsoft\systemcertificates\disallowed

Opens key

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus disallowed \setminus certificates$

HKCU\software\policies\microsoft\systemcertificates\disallowed\crls Opens key: Opens key: $HKCU \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus disallowed \setminus ctls$ Opens key $HKLM \verb|\software\m| icrosoft \verb|\systemcertificates\m| disallowed \verb|\certificates\m|$ ${\tt HKLM \ } . \\ {\tt software \ } . \\ {\tt icrosoft \ } . \\ {\tt systemcertificates \ } \\ {\tt disallowed \ } \\ {\tt crls}$ Opens key: ${\it HKLM} \verb|\software\microsoft\systemcertificates\disallowed\ctls$ Opens key: Opens key: HKLM\software\policies\microsoft\systemcertificates HKLM\software\policies\microsoft\systemcertificates\disallowed Opens key:

Opens key:

HKLM\software\policies\microsoft\systemcertificates\disallowed\certificates

HKLM\software\policies\microsoft\systemcertificates\disallowed\crls Opens kev: HKLM\software\policies\microsoft\systemcertificates\disallowed\ctls Opens key: Opens key: HKLM\software\microsoft\enterprisecertificates\disallowed\certificates Opens key: ${\tt HKLM \setminus software \setminus \dot microsoft \setminus enterprise certificates \setminus disallowed \setminus crls}$ Opens key: $HKLM \setminus software \setminus microsoft \setminus enterprise certificates \setminus disable wed \setminus ctls$ ${\tt HKCU \ } \dot{software \ } \dot{microsoft \ } system certificates \ \\ trust \ \\ physical stores$ Opens kev:

Opens key: HKCU\software\microsoft\systemcertificates\trust\

Opens key: ${\tt HKLM} \\ {\tt software} \\ {\tt microsoft} \\ {\tt systemcertificates} \\ {\tt trust} \\ {\tt physical stores} \\$

Opens key: HKLM\software\microsoft\systemcertificates\trust\

Opens key: HKLM\software\microsoft\enterprisecertificates\trust\physicalstores

Opens key: HKLM\software\microsoft\enterprisecertificates\trust

Opens key: $\label{prop:linear} \begin{tabular}{ll} HKCU \software \microsoft \system certificates \mbox{$\mbox{$my$} \physical stores} \end{tabular}$

Opens key: HKCU\environment

Opens key: HKCU\volatile environment

HKCU\software\microsoft\systemcertificates\my Opens key: HKCU\software\microsoft\systemcertificates\my\ Opens key: $\begin{tabular}{ll} HKCU \label{limits} LKCU \label{limits} Wy \label{limits} LKCU \label{limits} The constraint \label{limits} LKCU \label{limits} Wy \label{limits} LKCU \label{limits} Wy \label{limits} LKCU \label{limits} Wy \label{limits} Wy \label{limits} LKCU \label{limits} Wy \label{limits}$ Opens key:

Opens kev: $\label{local-objective} \mbox{HKCU\software\mbox{\sc microsoft\systemcertificates\mbox{\sc my\crls}} \\$ HKCU\software\microsoft\systemcertificates\my\ctls Opens kev: HKCU\software\microsoft\systemcertificates\my\keys Opens kev: Opens key: HKCU\software\microsoft\systemcertificates\root\certificates

Opens key: HKCU\software\microsoft\systemcertificates\root\crls Opens key: HKCU\software\microsoft\systemcertificates\root\ctls Opens key: HKLM\software\microsoft\systemcertificates\root\certificates Opens key: HKLM\software\microsoft\systemcertificates\root\crls

Opens key: HKLM\software\microsoft\systemcertificates\root\ctls Opens key: HKLM\software\microsoft\systemcertificates\authroot\certificates HKLM\software\microsoft\systemcertificates\authroot\crls Opens key:

HKLM\software\microsoft\systemcertificates\authroot\ctls Opens key: Opens key: HKLM\software\policies\microsoft\systemcertificates\root

Opens key: $\label{lem:hklm} \verb+Kklm/software/policies/microsoft/systemcertificates/root/certificates$ Opens key: HKLM\software\policies\microsoft\systemcertificates\root\crls

Opens key: HKLM\software\policies\microsoft\systemcertificates\root\ctls Opens key: $HKLM \setminus software \setminus microsoft \setminus enterprise certificates \setminus root \setminus certificates$ Opens key: HKLM\software\microsoft\enterprisecertificates\root\crls Opens key: HKLM\software\microsoft\enterprisecertificates\root\ctls Opens key: $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ systemcertificates \verb+ \trust \verb+ certificates \verb+ \\$ Opens key: $\label{lem:hkcu} \verb+KKCU\+software\+microsoft\+systemcertificates\+trust\+crls$

Opens kev: $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ systemcertificates \verb+ trust \verb+ ctls+ \\$ Opens kev: HKCU\software\policies\microsoft\systemcertificates\trust Opens key:

HKCU\software\policies\microsoft\systemcertificates\trust\certificates HKCU\software\policies\microsoft\systemcertificates\trust\crls Opens key: HKCU\software\policies\microsoft\systemcertificates\trust\ctls Opens key: HKLM\software\microsoft\systemcertificates\trust\certificates Opens kev: Opens key: HKLM\software\microsoft\systemcertificates\trust\crls

Opens key: HKLM\software\microsoft\systemcertificates\trust\ctls Opens key: HKLM\software\policies\microsoft\systemcertificates\trust

HKLM\software\policies\microsoft\systemcertificates\trust\certificates Opens key:

Opens key: HKLM\software\policies\microsoft\systemcertificates\trust\crls Opens key: HKLM\software\policies\microsoft\systemcertificates\trust\ctls HKLM\software\microsoft\enterprisecertificates\trust\certificates Opens key: HKLM\software\microsoft\enterprisecertificates\trust\crls Opens kev:

Opens key: HKLM\software\microsoft\enterprisecertificates\trust\ctls Opens key: HKCU\software\microsoft\systemcertificates\ca\certificates Opens key: HKCU\software\microsoft\systemcertificates\ca\crls Opens key: HKCU\software\microsoft\systemcertificates\ca\ctls

Opens key: HKCU\software\policies\microsoft\systemcertificates\ca Opens key: HKCU\software\policies\microsoft\systemcertificates\ca\certificates Opens key: $HKCU \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus ca \setminus crls$

Opens key: $\label{lem:hkcusoftware policies microsoft} HKCU \ software \ \ microsoft \ system certificates \ \ \ ca \ \ ctls$ Opens key: $HKLM \setminus software \setminus microsoft \setminus system certificates \setminus ca \setminus certificates$

 ${\tt HKLM \setminus software \setminus irrosoft \setminus system certificates \setminus ca \setminus crls}$ Opens key:

```
Opens key:
                                     HKLM\software\policies\microsoft\systemcertificates\ca
  Opens key:
                                     HKLM \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus ca \setminus certificates
  Opens key:
                                     \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ system certificates\+ ca\+ crls
                                     {\tt HKLM \setminus software \setminus policies \setminus microsoft \setminus system certificates \setminus ca \setminus ctls}
  Opens kev:
  Opens kev:
                                     HKLM\software\microsoft\enterprisecertificates\ca\certificates
  Opens key:
                                     HKLM\software\microsoft\enterprisecertificates\ca\crls
                                     {\tt HKLM \setminus software \setminus microsoft \setminus enterprise certificates \setminus ca \setminus ctls}
  Opens kev:
  Opens key:
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo
  Opens key:
                                    HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllimportpublickeyinfoex
  Opens key:
                                    HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdlimportpublickeyinfoex
  Opens key:
                                    HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllconvertpublickeyinfo
  Opens key:
                                    HKLM\software\microsoft\cryptography\oid\encodingtype
1\cryptdllconvertpublickeyinfo
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens key:
0\certdllverifycertificatechainpolicy
                                     HKLM\software\microsoft\cryptography\oid\encodingtype
  Opens key:
1\certdllverifycertificatechainpolicy
  Opens key:
                                     HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                     HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\treatas
                                     HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas
  Opens key:
                                    HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
  Opens key
00aa00bdce0b}\inprocserver32
                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
  Opens key
                                    HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
  Opens key
00aa00bdce0b}\inprocserverx86
  Opens kev:
                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86
  Opens key
                                    HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\localserver32
  Opens key:
                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver32
  Opens key
                                    HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprochandler32
  Opens kev:
                                    HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\ \ in prochandler 32
                                     HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-
  Opens key
00aa00bdce0b}\inprochandlerx86
                                     HKCR \verb|\clsid|{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprochandlerx86| | Color of the color
  Opens key
  Opens key
                                     HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82
00aa00bdce0b}\localserver
  Opens key:
                                     HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver
  Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iepeers.dll
  Opens key:
                                     HKCU\software\policies\microsoft\internet explorer\persistence
  Opens key
                                     \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ internet\ explorer\+ persistence
  Opens key:
                                     HKCU \setminus software \setminus classes \setminus typelib \setminus \{7e8bc440 - aeff-11d1 - 89c2 - 00c04fb6bfc4\}
                                     HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}
  Opens kev:
                                     HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
  Opens key:
                                     HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0
  Opens kev:
                                     HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
  Opens kev:
00c04fb6bfc4}\1.0\0
                                     HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0
  Opens key:
                                    HKCU\software\classes\typelib\{7e8bc440-aeff-11d1-89c2-
  Opens key
00c04fb6bfc4}\1.0\0\win32
  Opens key:
                                    HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32
  Opens key
                                     HKCU\software\classes\protocols\name-space handler\http\
  Opens key
                                     HKCR\protocols\name-space handler\http
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsperserve
                                     HKLM\software\microsoft\internet
  Opens key
explorer\main\featurecontrol\feature_maxconnectionsperserver
  Opens key
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_maxconnectionsper1_Oserver
  Opens key:
                                    HKLM\software\microsoft\internet
\verb|explorer| \verb|main| featurecontrol| feature_max connection sper 1\_0 server|
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\urlmon settings
  Opens key:
                                    HKCU\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
  Opens key:
                                    HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_include\_port\_in\_spn\_kb908209
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_disable_legacy_compression
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_legacy_compression
                                     HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_block_lmz_img
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_block_lmz_img
                                     HKLM\software\\macromedia\\flashplayerplugin
  Opens key:
                                     HKLM\software\policies\microsoft\internet explorer\recovery
  Opens key
                                     HKCU\software\microsoft\internet explorer\recovery
  Opens key
  Opens key:
                                     HKLM\software\microsoft\internet explorer\recovery
  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:
                                     HKCR\.png
  Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imgutil.dll
                                     HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
  Opens key:
  Opens key:
                                    HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}
```

HKLM\software\microsoft\systemcertificates\ca\ctls

Opens key:

```
Opens key:
                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\treatas
  Opens key:
                                            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas
  Opens key:
                                            HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\inprocserver32
                                            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32
  Opens kev:
                                            HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
  Opens key
00aa006c1a01}\inprocserverx86
                                            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserverx86
  Opens key:
  Opens key
                                            HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
00aa006c1a01}\localserver32
  Opens key:
                                            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver32
                                            HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
  Opens key
00aa006c1a01}\inprochandler32
                                            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\ \ inprochandler 32
  Opens key:
  Opens key
                                             HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724
00aa006c1a01}\inprochandlerx86
                                            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01\}\nprochandlerx86
  Opens kev:
                                            HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-
  Opens key
00aa006c1a01}\localserver
                                            HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver
  Opens key:
  Opens key
                                            HKCU \setminus software \setminus classes \setminus clsid \setminus \{6a01fda0-30df-11d0-b724-00aa006c1a01\}
  Opens key:
                                            HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}
  Opens key:
                                            HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\treatas
  Opens key:
                                             HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\treatas
  Opens key:
                                            HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
00aa006c1a01}\inprocserver32
                                             HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32
  Opens key:
                                            HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
  Opens key:
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 kev:
                                            HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
  Opens key
00aa006c1a01}\inprochandler32
                                            HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\linerochandler32
  Opens kev:
  Opens key:
                                            HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724
00aa006c1a01}\inprochandlerx86
  Opens key:
                                            HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\nprochandlerx86
                                            HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-
  Opens key
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
  Opens key
                                             HKCU\software\classes\mime\database\content type\image/bmp\bits
  Opens key:
                                             HKCR\mime\database\content type\image/bmp\bits
  Opens key:
                                             \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \classes \mime \database \content type \sime \database \content type \classes \mime \database \content type \classes \mime \classes \mime \database \content type \sime \classes \mime 
  Opens key:
                                             {\tt HKCR\mbox{\tt mime}\database\content\ type\limage/gif\bits}
  Opens kev:
                                             HKCU\software\classes\mime\database\content type\image/jpeg\bits
  Opens kev:
                                             HKCR\mime\database\content type\image/jpeg\bits
  Opens key:
                                             HKCU\software\classes\mime\database\content type\image/pjpeg\bits
                                             HKCR\mime\database\content type\image/pjpeg\bits
  Opens kev:
  Opens kev:
                                             HKCU\software\classes\mime\database\content type\image/png\bits
  Opens key:
                                             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 key:
  Opens key:
                                             HKCU\software\classes\mime\database\content type\image/x-icon\bits
  Opens key:
                                             HKCR\mime\database\content type\image/x-icon\bits
  Opens key:
                                             HKCU\software\classes\mime\database\content type\image/x-jg\bits
  Opens key:
                                             HKCR\mime\database\content type\image/x-jg\bits
                                             HKCU\software\classes\mime\database\content type\image/x-png\bits
  Opens key:
  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
  Opens key
                                             HKCR\mime\database\content type\image/x-png
                                             HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
  Opens key:
  Opens key
                                            HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}
  Opens key:
                                             HKCU \setminus software \setminus classes \setminus clsid \setminus \{a3ccedf7-2de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-12de2-11d0-86f4-10d0-86f4-10d0-86f4-10d0-86f4-10d0-86f4-10d0-86f4-10d0-86f4-10d0-86f4-10d0-86f4-10d0-86f4-10d0-
00a0c913f750}\treatas
                                             HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\treatas
  Opens key:
  Opens key
                                            HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprocserver32
                                            HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32
  Opens key:
                                            HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
  Opens key
00a0c913f750}\inprocserverx86
                                            HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86
  Opens key:
  Opens key:
                                            HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\localserver32
  Opens key:
                                            HKCR\clsid\a3ccedf7-2de2-11d0-86f4-00a0c913f750\\\localserver32
  Opens key:
                                            HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandler32
                                            HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\
  Opens key:
   Opens key
                                             HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
00a0c913f750}\inprochandlerx86
  Opens key:
                                            HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\) in prochandler x86
                                             HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-
  Opens key
00a0c913f750}\localserver
   Opens key:
                                             HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\localserver
  Opens key:
                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
```

HKCU\software\microsoft\cryptography\providers\type 024

options\pngfilt.dll
 Opens key:

```
Opens key:
                                          HKLM\software\microsoft\cryptography\defaults\provider types\type 024
  Opens key:
                                          enhanced rsa and aes cryptographic provider (prototype)
  Opens key:
                                          HKCU\software\microsoft\internet explorer\ietld\lowmic
  Opens key
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\historv\adobe.com
                                          HKCU\software\microsoft\internet
  Opens kev:
\hbox{\tt explorer$^{\cdot}$ main$ feature control $$ feature\_bypass\_cache\_for\_credpolicy\_kb936611$ }
  Opens key:
                                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
  Opens key:
                                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature ignore mappings for credpolicy
  Opens key:
                                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
  Opens key:
                                          HKCU\software\microsoft\internet explorer\searchproviders\
  Queries value:
                                          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Oueries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparentenabled]
                                          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
  Queries value:
                                          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                                          HKLM\software\microsoft\windows
  Oueries value:
\verb|nt\currentversion\compatibility| 32[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63]| 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 1
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63]
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:
                                          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
                                          {\it HKLM} \verb|\system| current controlset| control \verb|\session| \\
  Oueries value:
manager[criticalsectiontimeout]
                                          HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Oueries value:
                                          HKCR\interface[interfacehelperdisableall]
  Queries value:
  Oueries value:
                                          HKCR\interface[interfacehelperdisableallforole32]
  Oueries value:
                                          HKCR\interface[interfacehelperdisabletypelib]
                                          HKCR\interface\{00020400-0000-0000-c000-
  Oueries value:
00000000046}[interfacehelperdisableall]
  Oueries value:
                                          HKCR\interface\{00020400-0000-0000-c000-
00000000046} [interfacehelperdisableallforole32]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
   Queries value:
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
   Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
   Queries 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]
  Queries value:
                                          HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 7]
  Oueries value:
                                          HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 8]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Queries value:
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
   Queries value:
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
   Queries value:
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
   Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Oueries value:
HKLM \label{lem:hklm} In the label{lem:hklm} HKLM \label{lem:hklm} whe control \label{lem:hklm} In the label{lem:hklm} whe control \label{lem:hklm} In the label{lem:hklm} label{lem:hklm} whe control \label{lem:hklm} label{lem:hklm} labe
  Oueries value:
                                          HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer]
                                          HKI M\software\microsoft\windows nt\currentversion\drivers32[mixer1]
  Oueries value:
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Oueries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer51
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
  Queries value:
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
  Queries value:
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
  Queries value:
                                          HKCU\control panel\desktop[multiuilanguageid]
  Queries value:
                                          HKCU\control panel\desktop[smoothscroll]
  Oueries value:
Queries value:
                                          HKLM\system\setup[systemsetupinprogress]
   Queries value:
                                          HKLM\software\microsoft\ctf\systemshared[cuas]
  Queries value:
                                          HKCU\keyboard layout\toggle[language hotkey]
  Oueries value:
                                          HKCU\keyboard layout\toggle[hotkey]
  Queries value:
                                          HKCU\keyboard layout\toggle[layout hotkey]
   Queries value:
                                          HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:
                                          HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
  Queries value:
                                          HKCU\software\microsoft\ctf[disable thread input manager]
```

 $\label{lem:hkcu} \verb+kkcu+ software+ \verb+microsoft+ windows+ current version+ the memanager [compositing]$

HKCU\control panel\desktop[lamebuttontext]

Oueries value:

```
Oueries value:
                         HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
 Oueries value:
                         HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
 Oueries value:
                         HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
 Queries value:
                         HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
 Oueries value:
                         HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
 Oueries value
HKLM\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewwatermark]
 Queries value:
Queries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{listviewshadow} \end{tabular}
 Oueries value:
Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
                         HKLM\software\microsoft\windows\currentversion[programfilesdir]
 Queries value:
 Oueries value:
\label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
 Oueries value:
Oueries value
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
 Queries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [no set folders]
                         HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
 Oueries value:
 Oueries value:
                         HKLM\svstem\wpa\pnp[seed]
 Queries value:
                         HKLM\system\setup[osloaderpath]
 Queries value:
                         HKLM\system\setup[systempartition]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus setup [service pack cachepath]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
  Queries value:
                         HKLM\software\microsoft\windows\currentversion[devicepath]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\setup[loglevel]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\setup[logpath]
 Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Oueries value:
                         {\tt HKLM \ } system \verb| current control set \verb| services \verb| tcpip \verb| parameters [host name] \\
 Oueries value:
                         \label{lem:hklm} \verb+Kklm \system \current control set \services \tcpip \parameters [domain]
 Oueries value:
                         HKLM\software\microsoft\rpc[maxrpcsize]
 Oueries value:
11e3-9fc7-806d6172696f}[data]
 Oueries value:
11e3-9fc7-806d6172696f}[generation]
 Queries value:
HKCU \ software \ microsoft \ windows \ current version \ policies \ explorer [dontshow superhidden]
                         HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Queries value:
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
 Queries value
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
 Oueries value
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
 Queries value
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
 Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Queries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
 Queries value:
                         \label{thm:cosoftware} \begin{tabular}{ll} HKCU \software \mbox{$\stackrel{\cdot}{\rm microsoft}$} \windows \current version \explorer \advanced [filter] \end{tabular}
 Queries value:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced [show superhidden]} \end{tabular}
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
```

```
Oueries value:
\label{thm:linear} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \explorer \advanced [nonetcrawling] \end{tabular}
    Oueries value:
                                                                HKCR\directory[docobject]
     Oueries value:
                                                                HKCR\directory[browseinplace]
    Oueries value:
                                                                HKCR\directory[isshortcut]
    Oueries value:
                                                                HKCR\directory[alwaysshowext]
    Oueries value:
                                                                HKCR\directory[nevershowext]
    Oueries value:
                                                                HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
    Oueries value:
                                                                HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]
                                                                HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
    Oueries value:
409d6c4515e9}[drivemask]
    Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
    Queries value:
                                                                HKCR\.exe[]
    Queries value:
                                                                HKCR\exefile[docobject]
    Queries value:
                                                                HKCR\exefile[browseinplace]
    Queries value:
                                                                HKCR\exefile[isshortcut]
    Oueries value:
                                                                HKCR\exefile[alwaysshowext]
     Queries value:
                                                                HKCR\exefile[nevershowext]
     Queries value:
                                                                HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders[personal]
    Oueries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [used esktopinicache]
    Oueries value:
                                                                \label{lem:hklmsoftware} \verb+MKLM\+ software \verb+\microsoft+ windows \verb+\current version+ explorer \verb+\user+ shell+ explorer expl
 folders[common documents]
    Queries value:
                                                                \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ explorer \verb+ user shell
 folders[desktop]
    Queries value:
                                                                HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common desktop]
                                                                HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
    Oueries value:
                                                                HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
    Queries value:
00c04fd91972}\inprocserver32[loadwithoutcom]
    Oueries value:
                                                                HKCR\.asp[1
    Oueries value:
                                                                HKCR\.bat[]
                                                                HKCR\.cer[]
    Oueries value:
    Queries value:
                                                                HKCR\.chm[]
    Queries value:
                                                                HKCR\.cmd[]
    Oueries value:
                                                                HKCR\.com[1
    Oueries value:
                                                                HKCR\.cpl[1
     Queries value:
                                                                HKCR\.crt[]
    Queries value:
                                                                HKLM\software\microsoft\com3[com+enabled]
     Queries value:
                                                                HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
     Queries value:
                                                                HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
                                                                HKLM\software\microsoft\com3[regdbversion]
     Queries value:
    Queries value:
                                                                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
    Queries value:
                                                                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
    Queries value:
                                                                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
    Oueries value:
                                                                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
    Queries value
                                                                HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
                                                                HKLM\software\microsoft\internet
    Oueries value:
explorer\main\featurecontrol\feature protocol lockdown[755a4b2ec15da6bb01248b2dfbad206c340ba937eae9c35f04f6cedfe5e99d63.exe]
                                                                HKLM\software\microsoft\internet
    Oueries value:
explorer\main\featurecontrol\feature_protocol_lockdown[*]
    Queries value:
                                                                HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
    Queries value:
                                                                HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
    Queries 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:
                                                                HKLM\software\microsoft\windows\currentversion\internet
 settings[enablepunycode]
                                                                HKLM\software\policies\microsoft\internet
    Queries value:
explorer\security[disablesecuritysettingscheck]
    Queries value:
                                                                HKCU\software\microsoft\windows\currentversion\internet
 settings\zones\0[flags]
    Oueries value:
                                                                HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
    Queries value:
                                                                HKCU\software\microsoft\windows\currentversion\internet
 settings\zones\2[flags]
    Queries value:
                                                                HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
                                                                HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
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 main| feature method feat
    Queries value:
                                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
                                                                HKCU\software\microsoft\windows\currentversion\internet
    Queries value
 settings[specialfolderscachesize]
                                                                HKLM\software\microsoft\windows\currentversion\internet
    Queries value:
 settings[specialfolderscachesize]
    Queries value:
                                                                HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders[cache]
    Oueries value:
                                                                \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ explorer \verb+ user shell
folders[cookies]
```

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

settings\zones\0[1806]

Oueries value: HKCR\exefile\shell\open\command[] Oueries value: HKCR\exefile\shell\open\command[command]

Oueries value: HKCU\software\microsoft\windows\shellnoroam\muicache[langid] HKCU\software\microsoft\windows\shellnoroam\muicache[c:\program Oueries value:

files\flashplayer18_a_install.exe]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]

Oueries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]

Queries value:

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \policies \explorer[disallow run] \end{tabular}$

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[norunasinstallprompt]

Oueries value:

HKLM\system\currentcontrolset\control\session

manager\appcompatibility[disableappcompat]

Queries value: HKLM\system\wpa\mediacenter[installed]

Oueries value:

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

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

Oueries value: Oueries value:

be2efd2c1a33}[itemdata]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-

be2efd2c1a33}[saferflags] Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[itemdata]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde1328}[hashalg1

Queries value:

edd5fbde1328}[itemsize]

Oueries value:

edd5fbde1328}[saferflags]

b813f72dbb91}[itemdata]

Queries value:

b813f72dbb91}[hashalg]

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus (94e3e076-8f53-42a5-8411-144) + (14e3e076-8f53-42a5-8411-144) + (14e3e076-8f53-864) + (14e3e076-8f56-8f56) + (14e3e076-8f56-8f56) + (14e3e076-8f56-8f56) + (14e3e076-8f56-8f56) + (14e3e076-8f56-8f56) + ($

085bcc18a68d}[itemsize]

Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-

085bcc18a68d}[saferflags] Queries value:

b91490411bfc}[itemdata]

Queries value:

 $HKLM \label{lem:hklm} Which is the like of the like$ b91490411bfc}[hashalg]

Oueries value:

b91490411bfc}[itemsize] Queries value

b91490411bfc}[saferflags] Queries value:

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

Queries value:

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

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

```
folders[cache]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
    Oueries value:
                                                      {\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus app}
paths\install.exe[runascommand]
                                                      HKCU\software\microsoft\windows\shellnoroam\muicache[c:\program
    Oueries value:
files\install.exel
                                                      HKLM\software\microsoft\windows\currentversion\app
   Oueries value:
paths\install.exe[useshortname]
                                                      HKLM\software\microsoft\windows\currentversion\app
   Oueries value:
paths\install.exe[appendpath]
                                                      HKLM\software\microsoft\windows\currentversion\app
   Queries value:
paths\install.exe[path]
                                                      HKLM\software\microsoft\windows\currentversion\app
    Queries value:
paths\install.exe[runasonnonadmininstall]
    Queries value:
                                                       HKLM\software\microsoft\windows
nt\currentversion\compatibility32[flashplayer18_a_install]
    Oueries value:
                                                      HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[flashplayer18_a_install]
    Queries value
                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe[debugger]
    Oueries value:
                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
options\install.exe[executeoptions]
   Queries value:
                                                      \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current version + image + file + execution + image + file + image +
options\install.exe[disableheaplookaside]
    Oueries value:
                                                      \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the constant \end{tabular} in the 
options\install.exe[shutdownflags]
   Queries value:
                                                      \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\install.exe[minimumstackcommitinbytes]
                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
   Queries value:
options\install.exe[globalflag]
                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
   Queries value:
options\install.exe[debugprocessheaponly]
                                                      HKLM\software\microsoft\windows nt\currentversion\image file execution
   Oueries value:
options\install.exe[applicationgoo]
                                                      HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\compatibility32[install]
   Oueries value:
                                                      HKLM\software\microsoft\windows nt\currentversion\ime
compatibilitv[install]
    Queries value:
                                                       HKCU\software\microsoft\windows\currentversion\policies\explorer[norun]
    Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \policies \explorer [nodrives] \end{tabular}
    Queries value
\label{thm:linear} \begin{tabular}{ll} HKCU \software \mbox{$\mathbb{N}$ indows \current version \policies \explorer [nonetconnect disconnect] } \end{tabular}
    Queries value
Oueries value
HKCU\software\microsoft\windows\currentversion\policies\explorer[noclose]
    Oueries value:
                                                      HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
    Oueries value:
                                                      HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
    Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
                                                      HKCR\clsid\{00bb2765-6a77-11d0-a535-
   Queries value:
00c04fd7d062}\inprocserver32[inprocserver32]
                                                      HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
    Queries value:
                                                      HKCR\clsid\{00bb2765-6a77-11d0-a535-00c04fd7d062}[appid]
    Queries value:
    Queries value:
                                                      HKCR\clsid\{00bb2765-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
                                                      HKCR\clsid\{8856f961-340a-11d0-a96b-
    Queries value
00c04fd705a2}\inprocserver32[inprocserver32]
    Queries value:
                                                      \label{lem:hkcrclsid} $$HKCR\clsid_{8856f961-340a-11d0-a96b-00c04fd705a2} \in \clsid_{8856f961-340a-11d0-a96b-00c04fd705a2} inprocessing the second s
    Queries value:
                                                      HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[appid]
    Queries value:
                                                      HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
    Oueries value:
                                                      HKCR\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[inprocserver32]
                                                      HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]
    Oueries value:
    Queries value:
                                                      HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
    Queries value:
                                                      HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
    Oueries value:
                                                      HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
                                                      HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[appid]
    Queries value:
    Queries value:
                                                      HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
    Queries value:
                                                      HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-00000000000000]
                                                      HKCR\clsid\{03c036f1-a186-11d0-824a-
    Queries value:
00aa005b4383}\inprocserver32[threadingmodel]
    Oueries value:
                                                      HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
    Queries value:
                                                      HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
    Queries value:
                                                      HKLM\software\microsoft\internet explorer\setup[installstarted]
    Queries value:
                                                      HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
    Queries value:
                                                      HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\nprocserver32[]
    Queries value:
                                                       Queries value:
                                                       Oueries value:
                                                      Queries value:
                                                      HKCR\interface \ \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\}\ proxystubclsid32[]
```

```
Oueries value:
                                     HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[appid]
  Oueries value:
                                     HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[alwaysdropup]
  Oueries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[flashplayer18_a_install.exe]
                                     HKCU\software\microsoft\internet explorer\main[frametabwindow]
  Oueries value:
  Oueries value:
                                     HKLM\software\microsoft\internet explorer\main[frametabwindow]
                                     HKCU\software\microsoft\internet explorer\main[framemerging]
  Oueries value:
  Queries value:
                                     HKLM\software\microsoft\internet explorer\main[framemerging]
                                     HKCU\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:
                                     HKLM\software\microsoft\internet explorer\main[sessionmerging]
  Queries value:
  Queries value:
                                     HKCU\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:
                                     HKLM\software\microsoft\internet explorer\main[admintabprocs]
  Queries value:
                                     HKLM\software\policies\microsoft\internet explorer\main[tabprocgrowth]
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\main[tabprocgrowth]
  Oueries value:
                                     HKLM\software\microsoft\internet explorer\main[tabprocgrowth]
                                     HKLM\software\microsoft\internet explorer\main[navigationdelay]
   Queries value:
   Queries value:
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-
   Oueries value:
08002b30309d}\inprocserver32[loadwithoutcom]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
                                     HKCU\software\microsoft\windows\currentversion\shell
  Queries value
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
  Queries value:
\label{prop:linear_loss} HKCU \software \mbox{\sc urrentversion} policies \explorer [enforces hell extension security] and the properties of the propertie
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\shell
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0x4011
                                     HKCU\software\microsoft\windows\currentversion\shell
  Queries value:
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}
0x4011
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-
  Oueries value:
08002b30309d}\inprocserver32[inprocserver32]
  Oueries value:
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]
  Oueries value
                                     HKCR\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\inprocserver32[threadingmodel]
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
                                     HKLM\software\policies\microsoft\internet
  Queries value:
explorer\main[security_hklm_only]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[certificaterevocation]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries 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]
                                     \label{lem:hkcu} \begin{tabular}{ll} HKCU \end{tabular} windows \current version \end{tabular} internet
  Queries value:
settings[enablenegotiate]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[disablebasicoverclearchannel]
  Queries value:
                                     HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol[feature\_clientauthcertfilter]| \\
  Queries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Oueries value:
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[clientauthbuiltinui]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
  Oueries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings \verb|\| 5.0 \verb|\| cache[sessionstarttimedefaultdeltasecs]|
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\content[peruseritem]
                                     HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
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]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
                                     HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
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
```

HKLM\software\microsoft\windows\currentversion\internet

settings\5.0\cache\history[peruseritem]

```
settings\5.0\cache\history[peruseritem]
      Oueries 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
     Oueries value:
settings\5.0\cache\history[cachelimit]
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
     Oueries value:
settings\5.0\cache\extensible cache\domstore[cacherepair]
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
     Oueries value:
settings\5.0\cache\extensible cache\domstore[cachepath]
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
     Queries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
     Queries value:
settings\5.0\cache\extensible cache\domstore[cachelimit]
      Queries value:
                                                                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
 settings\5.0\cache\extensible cache\domstore[cacheoptions]
      Oueries value
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\feedplat[cacherepair]
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\feedplat[cachepath]
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
     Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
     Queries 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]
     Queries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
     Oueries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
     Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
     Oueries 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]
      Queries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\ietld[cacheprefix]
      Queries value
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
      Queries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
     Queries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012014033120140407[cacherepair]|
     Queries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
     Oueries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
     Oueries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[requiredfile]
      Queries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[version]
     Queries value:
HKLM \label{lem:hklm} Which is the like the li
      Queries value:
Queries value:
HKLM \label{lem:hklm} Which is the like the li
      Queries value
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
      Queries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
     Oueries value:
settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012014041220140413| [cacherepair]|
     Oueries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
     Oueries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
      Oueries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[win95defview]
      Oueries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[docobject]
     Queries value:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\install.exe[flushnowaitalways]
     Queries value:
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ install. exe[mycomputerfirst]
     Oueries value:
HKLM \label{lem:hklm} Which is the limit of the limit o
      Oueries value:
\label{thm:hammon} HKL^{\tt MKLM} (a) the three 
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ 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} \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} \label{lklm} \labell} \label{lklm} \label{lklm} \labell{lklm
      Queries value
HKLM \label{lem:hklm} Which is the like of the like 
      Queries value:
HKLM \ software \ `microsoft \ 'windows \ 'current version's hell compatibility \ 'applications \ 'install.exe[win95shlexec] \ 'exercise \ 'exercise
      Queries value:
                                                                                     HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
     Oueries value:
settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012014041220140413[ cache options]|
    Queries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\privacie:[cacherepair]
    Oueries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
    Oueries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
     Queries value:
HKLM \label{lem:hklm} Which is the like of the like 
     Queries value:
HKLM \label{lem:hklm} In the latest and the lates
     Oueries value
HKLM \label{lem:hklm} Which is the like of the like 
     Queries value
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ install. exe[ansidisplaynames]
     Oueries value
HKLM \label{lem:hklm} In the like the
     Oueries value
HKLM \ software \ \ install. exe[forcelfnidlist] \\
     Queries value
HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ applications \ in stall. exe \ starcraft
1.03[requiredfile]
     Queries value
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                                                                           HKLM\software\microsoft\windows\currentversion\internet
    Queries value:
settings[disableworkerthreadhibernation]
    Oueries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[socketsendbufferlength]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[socketreceivebufferlength]
     Oueries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
 settings[keepalivetimeout]
     Queries value:
                                                                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[maxhttpredirects]
     Queries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
 settings[maxconnectionsperserver]
                                                                           HKLM\software\microsoft\windows\currentversion\internet
     Queries value:
 settings[maxconnectionsperserver]
    Queries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
    Oueries value:
                                                                           HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
    Queries value
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[serverinfotimeout]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[connecttimeout]
                                                                           HKLM\software\microsoft\windows\currentversion\internet
    Queries value:
settings[connecttimeout]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[connectretries]
    Queries value:
                                                                           HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
     Queries value
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
     Queries value:
                                                                           HKLM\software\microsoft\windows\currentversion\internet
 settings[sendtimeout]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
     Queries value:
settings[receivetimeout]
     Queries value:
                                                                           HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
     Oueries value
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
    Queries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
{\tt settings[scavengecachelowerbound]}
    Queries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings\5.0\cache[scavengecachefilelifetime]
    Queries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                                                                           HKLM\software\microsoft\windows\currentversion\internet
    Queries value:
settings\5.0\cache[scavengecachefilelimit]
                                                                           HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[httpdefaultexpirytimesecs]
     Queries value
                                                                           HKCU\software\microsoft\windows\currentversion\internet
 settings[ftpdefaultexpirytimesecs]
                                                                           HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[flashplayer18_a_install.exe]
     Queries value
                                                                           HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                                                                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft + windows + current version + internet with the software \verb+microsoft + windows + current version + internet with the software \verb+microsoft + windows + current version + internet with the software + int
     Queries value
 settings[disablecachingofsslpages]
    Oueries value:
                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
```

```
\label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
   Oueries value:
settings[leashlegacycookies]
   Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
  Oueries value
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                                           HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dialupuselansettings]
  Oueries value
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypassftptimecheck]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[releasesocketduringauth]
  Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[releasesocketduring401auth]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
   Queries value
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
   Queries value
                                           \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
settings[disablelegacypreauthasserver]
                                            HKCU\software\microsoft\windows\currentversion\internet
   Queries value
settings[bypasshttpnocachecheck]
  Queries value:
                                            \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
{\tt settings[bypasshttpnocachecheck]}
  Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasssslnocachecheck]
  Oueries value
                                           HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[nocheckautodialoverride]
                                           HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
   Oueries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
   Queries value:
                                           \label{lem:hklm} \verb+ HKLM \+ software \+ microsoft \+ windows \+ current version \+ internet
settings[dontusednsloadbalancing]
   Queries value:
                                            HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                                            HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[mimeexclusionlistforcache]
  Queries value
                                            \label{local-continuous} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \\
settings[headerexclusionlistforcache]
  Oueries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value
                                            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[dnscachetimeout]
                                           HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnonpost]
  Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                                           \label{thm:local_equation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt definition} \
  Queries value:
settings[warnonzonecrossing]
                                           \label{lem:hkcu} \mbox{H\-\sc KCU\-} software\-\mbox{microsoft\-\windows\-\currentversion\-\sc internet}
  Queries value:
settings[warnonbadcertsending]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
   Queries value:
                                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
                                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Queries value
settings[alwaysdrainonredirect]
   Queries value:
                                            \label{lem:hkcu} \verb+KKCU\+ software\+ icrosoft\+ windows\+ current version\+ internet
settings[warnonhttpstohttpredirect]
   Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
   Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
   Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
   Queries value:
Queries value:
HKLM \label{lem:hklm} Which is a substitution of the latest and 
   Queries value
Queries value
Queries value
Oueries value
```

Oueries value: Oueries value: Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\00000000011[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num] Oueries value HKLM\svstem\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[librarypath] Queries value: Queries value: Oueries value: Queries value: $HKLM \label{lem:hklm} Which is the properties and the properties and the properties and the properties and the properties are larger and the properties ar$ Queries value: Queries value: Queries value: Queries value: Queries value: Queries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000002[addressfamily] Oueries 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\00000000002[version] Queries value: $HKLM \system \current controls et \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \names$ Queries value Queries value Queries value Oueries value: Oueries value HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace] Oueries value: $HKLM \ system \ \ current control set \ services \ \ winsock 2 \ parameters \ \ namespace_catalog5 \ \ \ catalog_entries \ \ \ 0000000000003 \ [enabled]$ Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[storesserviceclassinfo] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 spin count]$ Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[enableautodial] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings[urlencoding] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[truncatefilename] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[badproxyexpirestime] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nofilemenu] Queries value: HKCR\protocols\handler\res[clsid] HKCR\clsid\{3050f3bc-98b5-11cf-bb82-Oueries value: 00aa00bdce0b}\inprocserver32[inprocserver32] HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[] Queries value: HKCR\clsid\{3050f3bc-98b5-11cf-bb82-00aa00bdce0b}[appid] Queries value: HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_protocol_lockdown[install.exe] HKCR\clsid\{3050f3bc-98b5-11cf-bb82-Queries value: 00aa00bdce0b}\inprocserver32[threadingmodel] Oueries value: HKLM\software\microsoft\internet

Queries value: hkLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[flashplayer18_a_install.exe]
Queries value: hkLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_dispparams[*]
Queries value: hkLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[flashplayer18_a_install.exe]
Queries value: hkLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]
Queries value: hkLM\software\microsoft\internet explorer\application
compatibility[flashplayer18_a_install.exe]
Queries value: hkCU\software\microsoft\internet explorer\domstorage[totallimit]

```
Oueries value:
                         HKCU\software\microsoft\internet explorer\domstorage[domainlimit]
 Oueries value:
                         HKLM\software\microsoft\windows\currentversion\policies\ratings[key]
 Oueries value:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[install.exe]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[install.exe]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[urlencoding]
 Oueries value:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[flashplayer18_a_install.exe]
 Queries value:
                         HKCR\exefile\shell[]
                         HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[flashplayer18_a_install.exe]
 Oueries value:
Queries value:
                         HKCU\software\microsoft\internet explorer[no3dborder]
                         HKLM\software\microsoft\internet explorer[no3dborder]
 Oueries value:
                         HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_mime_handling[flashplayer18_a_install.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
  Oueries 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[*]
 Oueries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings[proxvenable]
 Oueries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[flashplayer18_a_install.exe]
 Queries value:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject[*]
 Oueries value:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[inprocserver32]
  Queries value:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[]
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid]
  Queries value:
 Queries value
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32[threadingmodel]
 Queries 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]
                         HKCR\clsid\{dd313e04-feff-11d1-8ecd-
 Oueries value:
0000f87a470c}\inprocserver32[inprocserver32]
 Oueries value:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature restrict filedownload[flashplayer18 a install.exel
                         HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_restrict_filedownload[*]
 Queries value:
                         HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[]
                         HKCR\protocols\handler\about[clsid]
 Queries value:
 Queries value:
                         HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}[appid]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\compatibility32[msmpeng]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[msmpeng]
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-
 Queries value
00aa00bdce0b}\inprocserver32[inprocserver32]
 Queries value:
                         HKCR \verb|\clsid|{3050f406-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprocserver32[]|
  Queries value:
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid]
 Oueries value:
                         HKCR\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprocserver32[threadingmodel]
 Oueries value:
006097deacf9}[version]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{5e6ab780-7743-11cf-a12b-
00aa004ae837}[version]
 Oueries value:
                         HKCR\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
 Queries value:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
 Queries value:
                         HKLM\software\microsoft\windows\currentversion\internet
settings\zones\3[2106]
 Queries value:
                         HKCU\software\microsoft\internet explorer\zoom[zoomdisabled]
 Oueries value:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]
 Oueries value:
                         HKLM\software\microsoft\internet explorer\registration[productid]
                         HKLM\software\policies\microsoft\internet explorer[smartdithering]
 Queries value:
  Queries value:
                         HKCU\software\microsoft\internet explorer[smartdithering]
 Queries value:
                         HKCU\software\microsoft\internet explorer[rtfconverterflags]
 Queries value:
                         HKLM\software\policies\microsoft\internet explorer\main[usecleartype]
                         HKCU\software\microsoft\internet explorer\main[usecleartype]
 Queries value:
 Queries value:
                         HKLM\software\policies\microsoft\internet
explorer\main[page_transitions]
  Queries value:
                         HKCU\software\microsoft\internet explorer\main[page_transitions]
```

HKLM\software\policies\microsoft\internet

Oueries value:

explorer\main[use_dlgbox_colors]

Oueries value: HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors] Oueries value: HKLM\software\policies\microsoft\internet explorer\main[anchor underline1 Oueries value: HKCU\software\microsoft\internet explorer\main[anchor underline] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[noinstrumentation] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{75048700-ef1f-11d0-9888-006097deacf9}\count[hrzr pgyfrffvba] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{5e6ab780-7743-11cf-a12b-00aa004ae837}\count[hrzr_pgyfrffvba] Queries value: HKCU\software\microsoft\internet explorer\main[css_compat] Oueries 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] HKLM\software\policies\microsoft\internet explorer\main[display inline Oueries value: videos] Queries value: HKCU\software\microsoft\internet explorer\main[display inline videos] Queries value: HKLM\software\policies\microsoft\internet explorer\main[play_background_sounds] Oueries value: HKCU\software\microsoft\internet explorer\main[play_background_sounds] Oueries value: $\label{lem:hklm} \verb+Kklm \+ software \+ policies \+ microsoft \+ internet explorer \+ main[play_animations]$ Queries value: HKCU\software\microsoft\internet explorer\main[play_animations] Oueries value: HKLM\software\policies\microsoft\internet explorer\main[print_background] HKCU\software\microsoft\internet explorer\main[print_background] Queries value: HKCU\software\microsoft\internet explorer\main[use stylesheets] Oueries value: HKLM\software\policies\microsoft\internet explorer\main[smoothscroll] Oueries value: Queries value: HKCU\software\microsoft\internet explorer\main[smoothscroll] Queries value: HKLM\software\policies\microsoft\internet explorer\main[xmlhttp] Oueries 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] Queries value: HKLM\software\policies\microsoft\internet explorer\main[disable script debugger] 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] Queries value: HKCU\software\microsoft\internet explorer\main[force offscreen composition] Queries value: HKLM\software\policies\microsoft\internet explorer\main[enable autoimageresize] Queries 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] Queries value: $HKCU \setminus software \setminus microsoft \setminus internet \ explorer \setminus main[q300829]$ Oueries value: HKCU\software\microsoft\internet explorer\main[cleanup htcs] HKLM\software\policies\microsoft\internet explorer\main[xdomainrequest] Oueries value: Oueries value: HKCU\software\microsoft\internet explorer\main[xdomainrequest] Oueries value: HKLM\software\microsoft\internet explorer\main[xdomainrequest] Oueries value: HKLM\software\policies\microsoft\internet explorer\main[domstorage] HKCU\software\microsoft\internet explorer\main[domstorage] Oueries value: HKLM\software\microsoft\internet explorer\main[domstorage] Queries value: HKCU\software\microsoft\internet Queries value: explorer\international[default_codepage] Queries value: HKCU\software\microsoft\internet explorer\international[autodetect] Queries value: HKCU\software\microsoft\internet explorer\international\scripts[default_iefontsizeprivate] Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color] Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color visited] Queries value: HKCU\software\microsoft\internet explorer\settings[anchor color hover] Queries value: HKCU\software\microsoft\internet explorer\settings[always use my colors] Queries value: HKCU\software\microsoft\internet explorer\settings[always use my font size] Oueries value: HKCU\software\microsoft\internet explorer\settings[always use my font face] Queries value: HKCU\software\microsoft\internet explorer\settings[disable visited hyperlinks] HKCU\software\microsoft\internet explorer\settings[use anchor hover Oueries value: color] Oueries value: HKCU\software\microsoft\internet explorer\settings[miscflags] Oueries value: HKCU\software\microsoft\windows\currentversion\policies[allow programmatic cut_copy_paste] HKLM\system\currentcontrolset\control\nls\codepage[950] Queries value: HKCU\software\microsoft\internet Queries value: explorer\international\scripts\3[iefontsize] Queries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iefontsizeprivate] HKCU\software\microsoft\internet Queries value: explorer\international\scripts\3[iepropfontname] Oueries value: HKCU\software\microsoft\internet explorer\international\scripts\3[iefixedfontname] Queries value: HKCU\software\microsoft\internet explorer\international[acceptlanguage] Queries value: HKLM\software\microsoft\internet explorer\version vector[vml] Oueries value: HKLM\software\microsoft\internet explorer\version vector[ie] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_zone_elevation[flashplayer18_a_install.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_zone_elevation[*]

HKCU\software\microsoft\windows\currentversion\internet

Queries value: settings\zones\0[2700]

```
Oueries value:
                                                          HKLM\software\microsoft\windows\currentversion\internet
settings\zones\0[2700]
   Oueries value:
                                                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[flashplayer18_a_install.exe]
   Oueries value:
                                                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature xssfilter[*]
   Oueries value:
                                                         HKCU\software\microsoft\windows\currentversion\internet
settings\zones[securitysafe]
   Oueries value:
                                                         HKCR\msxml2.domdocument.3.0\clsid[1
    Oueries value:
                                                         HKCR\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\inprocserver32[inprocserver32]
                                                         HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}\inprocserver32[]
    Queries value:
                                                         HKCR\clsid\{f5078f32-c551-11d3-89b9-0000f81fe221}[appid]
    Queries value:
    Queries value:
                                                         HKCR\clsid\{f5078f32-c551-11d3-89b9-
0000f81fe221}\inprocserver32[threadingmodel]
    Queries value:
                                                         HKU\.default\control panel\desktop[multiuilanguageid]
    Oueries value:
                                                         HKU\.default\control panel\desktop[smoothscroll]
    Oueries value:
                                                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[msmpeng.exe]
    Queries value:
                                                         HKLM\software\microsoft\windows
nt\currentversion\compatibility32[svchost]
    Oueries value:
                                                         HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[svchost]
    Queries value:
                                                         HKU\.default\software\microsoft\multimedia\audio[systemformats]
    Queries value:
                                                         HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.imaadpcm]
    Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
    Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
   Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
   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
    Oueries value
\label{thm:local_hamma} \begin{tabular}{ll} HKLM \end{tabular} \begin{tabular}{ll} HKLM \end{t
    Queries value:
Queries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
                                                          HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\drivers32[msacm.msg711]
    Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
   Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
   Oueries value
HKLM\software\microsoft\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]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
   Queries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus 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\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
    Queries value:
                                                         HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.trspch]
    Oueries value:
Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
    Queries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]
   Queries 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:
Queries value:
Oueries value:
HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msg 723 [cfilter tags]
                                                         HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msaudio1]
    Queries value
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msaudio1[cformattags]
    Queries value
HKLM \ "software \ "microsoft\ "audio compression manager \ "driver cache \ "msaudio 1 [a formattag cache] \\
```

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msaudio1[cfiltertags]$

Oueries value

HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.sl_anet] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport] Oueries value HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[cformattags] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[aformattagcache] Queries value: $HKLM \label{lem:hklm} In the latest and in the$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport] Oueries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.iac2 [cformattags]$ Queries value Oueries value HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.13acm] Oueries value: $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. 13 acm [fdw support]$ Queries value: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. 13 acm [cformattags]$ Queries value $HKLM \verb|\software\microsoft\audiocompression manager\driver cache\mbox{|} msacm. 13 acm [a formattag cache] \\$ Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags] Oueries value: HKU\.default\software\microsoft\multimedia\audio compression manager\msacm[nopcmconverter] HKU\.default\software\microsoft\multimedia\audio compression Queries value: manager\priority v4.00[priority1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[userenvdebuglevel] HKLM\software\microsoft\windows Oueries value: nt\currentversion\winlogon[chkaccdebuglevel] Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype] Oueries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user shell folders[personal] HKU\.default\software\microsoft\windows\currentversion\explorer\user Queries value: shell folders[local settings] HKLM\software\microsoft\windows Queries value: nt\currentversion\winlogon[rsopdebuglevel] HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] Queries value: 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: HKLM\software\microsoft\internet $explorer \verb|\main| featurecontrol| feature_protocol_lockdown[svchost.exe]|$ Oueries value: HKCU\software\microsoft\windows\currentversion\explorer[nofilefolderconnection] HKCR\directory\shellex\copyhookhandlers\cdf[]
HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32[] Oueries value: Oueries value: HKCR\clsid\{67ea19a0-ccef-11d0-8024-Oueries value: 00c04fd75d13}\inprocserver32[loadwithoutcom] HKLM\software\microsoft\windows\currentversion\shell Queries value: extensions\blocked[{67ea19a0-ccef-11d0-8024-00c04fd75d13}] HKCU\software\microsoft\windows\currentversion\shell Queries value: extensions\blocked[{67ea19a0-ccef-11d0-8024-00c04fd75d13}] Queries value: HKLM\software\microsoft\windows\currentversion\shell 0x4011 Queries value: HKCU\software\microsoft\windows\currentversion\shell Queries value: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32[inprocserver32] Oueries value: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}[appid] Oueries value: HKCR\clsid\{67ea19a0-ccef-11d0-8024-00c04fd75d13}\inprocserver32[threadingmodel] Oueries value: HKCR\directory\shellex\copyhookhandlers\filesystem[] HKCR\clsid\{217fc9c0-3aea-1069-a2db-08002b30309d}\inprocserver32[] Oueries value: Queries value: HKCR\directory\shellex\copyhookhandlers\mydocuments[] HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32[] Queries 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-c000-000000000046}} 0x4011 Queries value: HKCU\software\microsoft\windows\currentversion\shell extensions\cached[{ecf03a33-103d-11d2-854d-006008059367} {00000000-0000-0000-c000-0000000000046}} 0x401] HKCR\clsid\{ecf03a33-103d-11d2-854d-Queries value: 006008059367}\inprocserver32[inprocserver32] HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}[appid] Queries value:

Queries value: HKCR\clsid\{ecf03a33-103d-11d2-854d-006008059367}\inprocserver32[threadingmodel]
Queries value: HKCR\directory\shellex\copyhookhandlers\sharing[]
Queries value: HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}\inprocserver32[]
Queries value: HKCR\clsid\{40dd6e20-7c17-11ce-a804-

```
00aa003ca9f6}\inprocserver32[loadwithoutcom]
                                     HKLM\software\microsoft\windows\currentversion\shell
  Oueries value:
extensions\blocked[{40dd6e20-7c17-11ce-a804-00aa003ca9f6}]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{40dd6e20-7c17-11ce-a804-00aa003ca9f6}]
                                     HKLM\software\microsoft\windows\currentversion\shell
  Oueries value:
extensions\cached[{40dd6e20-7c17-11ce-a804-00aa003ca9f6} {00000000-0000-0000-c000-000000000046}}
0x4011
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\shell
0x401]
  Queries value:
                                     HKCR\clsid\{40dd6e20-7c17-11ce-a804-
00aa003ca9f6}\inprocserver32[inprocserver32]
  Queries value:
                                     HKCR\clsid\{40dd6e20-7c17-11ce-a804-00aa003ca9f6}[appid]
  Queries value:
                                     HKCR\clsid\{40dd6e20-7c17-11ce-a804-
00aa003ca9f6}\inprocserver32[threadingmodel]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
  Queries value:
                                     HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileimagepath]
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[fonts]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[startup]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ explorer \verb+ user shell
folders[programs]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[start menu]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[recent]
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[sendto]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
folders[nethood]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[printhood]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[templates]
  Queries value:
                                     \label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \label{lem:hklmsoftware} windows \current version \explorer \current version \current version \explorer \current version \explorer \current version \explorer \current version \current version \explorer \current version \explorer \current version \explorer \current version \current version \explorer \current \c
folders[common startup]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common programs]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\explorer\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]
  Oueries value:
                                     \label{lem:hklm} \verb+Kklm\+ software\+ windows\+ current version\+ explorer\+ user shell
folders[common appdata]
  Oueries value:
                                     HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common templates]
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Oueries value:
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]
                                     \label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[my pictures]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)]
                                     HKLM\software\microsoft\windows\currentversion[commonfilesdir]
   Queries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[administrative tools]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common administrative tools]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
  Oueries value:
                                     HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my music]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my video]
                                     HKLM\software\microsoft\windows\currentversion\explorer\user shell
  Oueries 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]
                                     HKLM\software\microsoft\windows\currentversion\explorer\user shell
  Queries value:
folders[oem links]
  Oueries value:
                                     HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cd burning]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[2106]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings\zones\0[2106]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\zones\0[1400]
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU\+software\+microsoft\+windows\+currentversion\+internet
settings[warnonintranet]
                                     HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
```

```
settings[warnonintranet]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
  Oueries value:
                                  HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
  Oueries value:
                                  HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid]
  Oueries value:
                                  HKCR\clsid\{50d5107a-d278-4871-8989-
  Oueries value:
f4ceaaf59cfc}\inprocserver32[threadingmodel]
                                  HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
  Oueries value:
c9633f71be64}\languageprofile\0x00000000\{63800dac-e7ca-4df9-9a5c-20765055488d}[enable]
  Queries value:
                                  HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32[inprocserver32]
  Queries value:
                                  HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]
                                  HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid]
  Queries value:
  Queries value:
                                  HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32[threadingmodel]
                                  HKCR\clsid\{a4b544a1-438d-4b41-9325-
  Oueries value:
869523e2d6c7}\inprocserver32[inprocserver32]
  Queries value:
                                  HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[]
  Queries value:
                                  HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]
  Oueries value:
                                  HKCR\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32[threadingmodel]
                                 HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
  Oueries value:
77e8f3d1aa80\} \land [description]
  Oueries value:
                                  77e8f3d1aa80\} \land (7ae86bb7-262c-431e-9111-c974b6b7cac3) [description]
                                 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
  Queries value:
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[description]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet settings\url
history[daystokeep]
                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
  Queries value:
00aa00bbbb58}\inprocserver32[inprocserver32]
  Oueries value:
                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[]
                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[appid]
  Oueries value:
  Queries value:
                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
  Oueries value:
                                  HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1201]
                                  HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:
  Queries value:
                                  HKLM\system\currentcontrolset\control\nls\language groups[1]
                                  HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:
  Queries value:
                                  HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[cointernetcombineiuricachesize]
  Queries value:
                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[cointernetcombineiuricachesize]
                                  HKCR\clsid\{81397204-f51a-4571-8d7b-
  Queries value:
dc030521aabd}\inprocserver32[inprocserver32]
  Oueries value:
                                  HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}\inprocserver32[]
                                  HKCR\clsid\{81397204-f51a-4571-8d7b-dc030521aabd}[appid]
  Oueries value:
                                  HKCR\clsid\{81397204-f51a-4571-8d7b-
  Oueries value:
dc030521aabd}\inprocserver32[threadingmodel]
                                 HKCR\clsid\{d1fe6762-fc48-11d0-883a-
  Oueries value:
3c8b00c10000}\inprocserver32[inprocserver32]
                                  HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}\inprocserver32[]
  Queries value:
  Queries value:
                                  HKCR\clsid\{d1fe6762-fc48-11d0-883a-3c8b00c10000}[appid]
                                  HKCR\clsid\{d1fe6762-fc48-11d0-883a-
  Queries value:
3c8b00c10000}\inprocserver32[threadingmodel]
  Queries value:
                                  HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_behaviors[flashplayer18\_a\_install.exe]|
  Queries value:
                                  HKLM\software\microsoft\internet
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:
                                 HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters[dhcpdomain]|
  Oueries value:
                                  HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
                                 HKCR\clsid\{4fd2a832-86c8-11d0-8fca-00c04fd9189d}\inprocserver32[]
  Oueries value:
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
  Oueries value:
c7d49d7cecdc}[leaseobtainedtime]
  Queries value:
c7d49d7cecdc}[leaseterminatestime]
  Queries value:
c7d49d7cecdc}[dhcpserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
  Oueries value:
                                  HKLM\software\microsoft\rpc\securityservice[10]
  Queries value:
Queries value:
                                  \label{local-equation-of-ca-00c04fd9189d} [appid] \\
  Queries value:
                                  HKCR \verb|\clsid| \{ 4fd2a832-86c8-11d0-8fca-
00c04fd9189d}\inprocserver32[threadingmodel]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
  Oueries value:
                           {\tt HKLM \ } system \verb| current control set \verb| services \verb| netbt \verb| parameters [node type]|
  Oueries value:
                           HKLM \verb|\system| current controlset \verb|\services| net bt \verb|\parameters[dhcpnodetype]|
  Oueries value:
                           HKLM\system\currentcontrolset\services\netbt\parameters[scopeid]
  Oueries value:
                           HKLM\system\currentcontrolset\services\netbt\parameters[dhcpscopeid]
  Oueries value:
                           HKLM\svstem\currentcontrolset\services\tcpip\parameters[ipenablerouter]
  Oueries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
  Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
  Queries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
  Queries value:
Queries value:
                           Oueries value:
                           HKLM\system\currentcontrolset\services\netbt\parameters[enableproxy]
  Oueries value:
                           HKLM\system\currentcontrolset\services\netbt\parameters[enabledns]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
  Queries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
  Oueries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
  Oueries value:
Queries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
  Oueries value:
                           HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Oueries value:
                           HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
                           HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
                           HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
  Oueries value:
  Oueries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
  Oueries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
  Oueries value:
                           HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [helperdllname]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
                           HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus msnsspc.dll[rpcid]
  Queries value:
  Queries value:
                           Oueries value:
                           HKLM \ system \ current control \ set \ control \ lsa \ sspic ache \ msnsspc. \\ dll[type]
  Queries value:
HKLM \verb|\system| current controlset \verb|\control| lsa \verb|\sspicache| msnsspc.dll[tokensize]|
  Oueries value:
                           HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
                           HKU\s-1-5-21-1757981266-507921405-1957994488-
  Oueries value:
1003\software\microsoft\windows nt\currentversion\winlogon[parseautoexec]
                           HKU\s-1-5-21-1757981266-507921405-1957994488-1003\control
 Oueries value:
panel\desktop[multiuilanguageid]
                           HKLM\hardware\devicemap\video[maxobjectnumber]
  Queries value:
  Queries value:
                           HKLM\hardware\devicemap\video[\device\video0]
  Queries value:
                           HKLM\hardware\devicemap\video[\device\video1]
  Queries value:
                           HKLM\hardware\devicemap\video[\device\video2]
  Queries value:
                           HKLM\software\microsoft\directdraw\compatibility\bug![name]
  Queries value:
                           HKLM\software\microsoft\directdraw\compatibility\bug![flags]
  Queries value:
                           HKLM\software\microsoft\directdraw\compatibility\bug![id]
                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus demolition derby 2 [name]
  Queries value:
  Queries value:
                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus demolition derby 2 [flags]
  Queries value:
                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus demolition derby 2 [id]
  Queries value:
                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus mortal kombat \\ 3[name]
  Oueries value:
                           HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[flags]
  Oueries value:
                           HKLM\software\microsoft\directdraw\compatibility\mortalkombat3[id]
  Oueries value:
                           HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\m| sgolf98[name]
  Oueries value:
                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus msgolf98[flags]
  Oueries value:
                           HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\m| sgolf98[id]
  Oueries value:
                           HKLM\software\microsoft\directdraw\compatibility\nhlpowerplay[name]
                           HKLM \verb|\software\m| icrosoft \verb|\directdraw\compatibility\nhlpowerplay[flags]|
  Oueries value:
                           Oueries value:
  Oueries value:
                           HKLM \setminus software \setminus microsoft \setminus direct draw \setminus compatibility \setminus norton system in fo[name]
  Oueries value:
                           HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[flags]
                           HKLM\software\microsoft\directdraw\compatibility\nortonsysteminfo[id]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\directdraw\compatibility\rogue squadron[name]
  Queries value:
                           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:
                           HKLM\software\microsoft\directdraw\compatibility\savage[flags]
  Oueries value:
                           HKLM\software\microsoft\directdraw\compatibility\savage[id]
                           HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[name]
  Oueries value:
                           HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[flags]
  Queries value:
  Queries value:
                           HKLM\software\microsoft\directdraw\compatibility\scorchedplanet[id]
  Queries value:
                           HKLM\software\microsoft\directdraw\compatibility\silentthunder[name]
  Oueries value:
                           HKLM\software\microsoft\directdraw\compatibility\silentthunder[flags]
  Queries value:
                           HKLM\software\microsoft\directdraw\compatibility\silentthunder[id]
  Queries value:
                           HKLM\software\microsoft\directdraw\compatibility\terracide[name]
  Queries value:
                           HKLM \ software \ `microsoft \ direct draw \ compatibility \ terracide [flags]
  Queries value:
                           HKLM\software\microsoft\directdraw\compatibility\terracide[id]
  Oueries 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\software\microsoft\directdraw\compatibility\thirddimension[id]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[name]
  Queries value
HKLM\software\microsoft\directdraw\compatibility\ziffdayisqualitybenchmark[flags]
  Oueries value
HKLM\software\microsoft\directdraw\compatibility\ziffdavisqualitybenchmark[id]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[name]
  Oueries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[flags]
  Queries value:
HKLM\software\microsoft\directdraw\compatibility\ziffdaviswinmarkbenchmark[id]
                                     HKLM\software\microsoft\directdraw[modexonly]
  Queries value:
  Queries value:
                                      HKLM\software\microsoft\directdraw[emulationonly]
  Queries value:
                                      HKLM\software\microsoft\directdraw[showframerate]
  Oueries value:
                                      HKLM\software\microsoft\directdraw[enableprintscreen]
  Oueries value:
                                      HKLM\software\microsoft\directdraw[forceagpsupport]
                                      HKLM\software\microsoft\directdraw[disableagpsupport]
   Queries value:
  Queries value:
                                      HKLM\software\microsoft\directdraw[disablemmx]
   Queries value:
                                      HKLM\software\microsoft\directdraw[disableddscapsinddsd]
  Oueries value:
                                      HKLM\software\microsoft\directdraw[disablewidersurfaces]
  Oueries value:
                                      HKLM\software\microsoft\directdraw[usenonlocalvidmem]
  Oueries value:
                                     HKLM \setminus software \setminus microsoft \setminus direct draw[forcerefreshrate]
  Queries value:
                                      HKLM\software\microsoft\direct3d[flipnovsync]
  Oueries value:
                                     HKU\s-1-5-21-1757981266-507921405-1957994488-
1003\software\microsoft\windows\currentversion\explorer\shell folders[cache]
                                     HKLM\software\microsoft\directdraw[owndc]
  Queries value:
  Oueries value:
                                     HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[inprocserver32]
                                     HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}\inprocserver32[]
  Queries value:
                                     HKCR\clsid\{a7ee7f34-3bd1-427f-9231-f941e9b7e1fe}[appid]
  Queries value:
  Oueries value:
                                     HKCR\clsid\{a7ee7f34-3bd1-427f-9231-
f941e9b7e1fe}\inprocserver32[threadingmodel]
                                     HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\compatibility32[dllhost]
  Oueries value:
                                     HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[dllhost]
  Oueries value:
                                      HKCR\dximagetransform.microsoft.gradient\clsid[]
                                     HKCR\clsid\{623e2882-fc0e-11d1-9a77-
   Queries value:
0000f8756a10}\inprocserver32[inprocserver32]
                                      HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}\inprocserver32[]
   Queries value:
   Queries value:
                                      HKCR\clsid\{623e2882-fc0e-11d1-9a77-0000f8756a10}[appid]
                                      HKCR\clsid\{623e2882-fc0e-11d1-9a77-
   Queries value:
0000f8756a10}\inprocserver32[threadingmodel]
                                     HKCU\software\microsoft\multimedia\audio[systemformats]
  Queries value:
  Queries value:
                                     \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ multimedia \verb+ audio compression \\
manager\msacm[nopcmconverter]
  Queries value:
                                     \label{thm:limedia} \textbf{HKCU} software \verb|\microsoft| multimedia \verb|\audio| compression manager \verb|\priority| \\
v4.00[priority1]
  Oueries value
                                     HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_protocol_lockdown[dllhost.exe]| \\
  Oueries value:
                                     HKU\.default\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
                                     HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[secureprotocols]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
                                     \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKU\label{thm:local_hammon} HKU\label{thm:local_hammon} \end{tabular} are $$\operatorname{HKU}\label{thm:local_hammon}.$$
  Queries value:
settings[certificaterevocation]
  Queries value:
                                     HKLM\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
  Queries value:
                                      HKU\.default\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
  Queries value:
                                      HKU\.default\software\microsoft\windows\currentversion\internet
settings[disablepassport]
                                      HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[idnenabled]
  Queries value:
                                     HKU\.default\software\microsoft\windows\currentversion\internet
settings[cachemode]
  Oueries value
                                      HKU\.default\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Queries value:
                                      HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Queries value:
                                      HKU\.default\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                                      HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[proxyhttp1.1]
  Queries value:
                                     HKU\.default\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
  Queries value:
                                     \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKU\label{thm:local_hammon} HKU\label{thm:local_hammon} \end{tabular} and the 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
settings[disablebasicoverclearchannel]
  Oueries value:
                                     HKCR\clsid\{c6365470-f667-11d1-9067-
00c04fd9189d}\inprocserver32[inprocserver32]
  Queries value:
                                     HKU\.default\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
                                      HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[syncmode5]
                                      HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}\inprocserver32[]
  Queries value:
  Queries value:
                                     \label{lem:hkuldefault} $$HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
  Queries value:
                                     \label{lem:hkul.default} HKU\.default\software\microsoft\windows\currentversion\sline internet
settings\5.0\cache\content[peruseritem]
                                     HKU\s-1-5-21-1757981266-507921405-1957994488-
  Queries value:
```

```
1003\software\microsoft\windows\currentversion\explorer\user shell folders[cache]
                                                               HKCR\clsid\{c6365470-f667-11d1-9067-00c04fd9189d}[appid]
     Oueries value:
    Oueries value:
                                                               HKCR\clsid\{c6365470-f667-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-9067-11d1-906
00c04fd9189d}\inprocserver32[threadingmodel]
    Queries value
                                                               HKCR\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[inprocserver32]
                                                               HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}\inprocserver32[]
    Oueries value:
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
    Oueries value:
settings\5.0\cache\content[cacheprefix]
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
    Oueries value:
settings\5.0\cache\content[cachelimit]
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
    Queries 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]
    Queries value:
                                                               HKCR\clsid\{4cb26c03-ff93-11d0-817e-0000f87557db}[appid]
    Oueries value
                                                               HKCR\clsid\{4cb26c03-ff93-11d0-817e-
0000f87557db}\inprocserver32[threadingmodel]
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\cookies[cacheprefix]
                                                                HKU\.default\software\microsoft\windows\currentversion\internet
    Queries value:
settings\5.0\cache\cookies[cachelimit]
    Queries value:
                                                               HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
 settings\5.0\cache\history[peruseritem]
                                                                HKU\s-1-5-21-1757981266-507921405-1957994488-
    Queries value:
 1003\software\microsoft\windows\currentversion\explorer\user shell folders[history]
    Queries value:
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\history[cacheprefix]
    Queries value:
                                                                HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
    Queries value:
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 \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
    Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
    Oueries value
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\ietld[cacheoptions]
    Queries value:
                                                               \label{lem:hkuldefault} $$HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012013122320131224[cacherepair]
    Queries value
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
 settings\5.0\cache\extensible cache\mshist012013122320131224[cachepath]
                                                               \label{thm:linear} \begin{tabular}{ll} HKU\label{thm:linear} AKU\label{thm:linear} AKU
    Queries value
 settings\5.0\cache\extensible cache\mshist012013122320131224[cacheprefix]
    Queries value
                                                               HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet| in the constant of 
settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012013122320131224[cache limit]|
    Oueries value:
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012013122320131224[cacheoptions]
    Oueries value
                                                               HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
f4fc1e6ca1bd}\inprocserver32[inprocserver32]
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[disableworkerthreadhibernation]
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[disablereadrange]
    Queries value:
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
                                                               HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}\inprocserver32[]
    Queries value:
                                                                HKU\.default\software\microsoft\windows\currentversion\internet
    Queries value:
settings[socketreceivebufferlength]
    Queries value:
                                                               \label{lem:hkul.default} HKU\.default\software\microsoft\windows\currentversion\sline internet
 settings[keepalivetimeout]
    Queries value:
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
 settings[maxhttpredirects]
    Queries value:
                                                               HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
 settings[maxconnectionsperserver]
                                                               HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
    Oueries value:
settings[maxconnectionsper1_0server]
    Queries value:
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                                                               HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-f4fc1e6ca1bd}[appid]
    Oueries value:
    Queries value:
                                                               HKCR\clsid\{385a91bc-1e8a-4e4a-a7a6-
 f4fc1e6ca1bd}\inprocserver32[threadingmodel]
    Oueries value:
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
 settings[serverinfotimeout]
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
    Queries value:
settings[connecttimeout]
                                                                HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
    Queries value:
settings[connectretries]
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
    Queries value:
 settings[sendtimeout]
    Queries value:
                                                               HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
 settings[receivetimeout]
    Queries value:
                                                               HKU\.default\software\microsoft\windows\currentversion\internet
 settings[disablentlmpreauth]
    Queries value:
                                                               HKU\.default\software\microsoft\windows\currentversion\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]
    Queries value:
                                                               HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet| in the constant of 
{\tt settings \ 1.0 \ cache[scavengecachefile limit]}
```

```
HKCR\typelib\{5e77eb03-937c-11d1-b047-00aa003b6061}\1.1\0\win32[]
   Oueries value:
   Oueries value:
                                              HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings[httpdefaultexpirytimesecs]
   Queries value
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Oueries value:
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[svchost.exe]
                                              HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disablecachingofsslpages]
                                              HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablecachingofsslpages]
                                              HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[perusercookies]
                                              HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
  Queries value:
settings[leashlegacycookies]
   Queries value:
                                              \label{lem:hkuldefault} $$HKU\.default\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
   Oueries value
                                              HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings[dialupuselansettings]
   Queries value
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
   Oueries value:
                                              \label{lem:hkuldefault} $$HKU\.default\software\microsoft\windows\currentversion\internet
settings[bypassftptimecheck]
  Queries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
  Queries value:
                                              \label{lem:hkul.default} HKU\label{lem:hkul.default} HKU\label{lem:hkul.default} Lem \label{lem:hkul.default} HKU\label{lem:hkul.default} Lem \label{lem:hkul.default} Lem \label{lem:hkul.d
settings[releasesocketduring401auth]
                                              HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value
settings[wpadsearchalldomains]
  Queries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
                                              HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[bypasshttpnocachecheck]
                                              HKU\.default\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[bvpasssslnocachecheck]
                                              HKU\.default\software\microsoft\windows\currentversion\internet
  Queries value:
settings[nocheckautodialoverride]
  Queries value:
                                              HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings[dontusednsloadbalancing]
   Queries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
   Queries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
   Queries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
   Queries value:
                                              HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet|
settings[dnscacheentries]
   Queries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Oueries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Oueries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
  Queries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[warnonbadcertsending]
  Queries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
                                              \label{lem:hkul} \verb|HKU|.default\software\microsoft\windows\currentversion\internet|
   Queries value:
settings[warnonpostredirect]
   Queries value:
                                              \label{thm:linear} \begin{tabular}{ll} HKU\label{thm:linear} AKU\label{thm:linear} AKU
settings[alwaysdrainonredirect]
                                              HKU\.default\software\microsoft\windows\currentversion\internet
   Queries value
settings[warnonhttpstohttpredirect]
   Queries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
   Oueries value
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[enableautodial]
  Oueries value:
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
  Queries value
                                              HKU\.default\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
  Queries value
                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[svchost.exe]
                                              HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
   Oueries value:
   Queries value:
Queries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus telephony [tapi32 request retry time out]
                                              HKLM\software\microsoft\tracing[enableconsoletracing]
   Queries value:
                                              HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
   Queries value:
   Oueries value:
                                              HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
   Oueries value:
                                              HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
   Queries value:
                                              HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
   Queries value:
                                              HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
                                              HKLM\software\microsoft\tracing\rasapi32[filedirectory]
   Queries value:
                                              HKCR\typelib\{54314d1d-35fe-11d1-81a1-0000f87557db}\1.1\0\win32[]
   Queries value:
                                              HKU\s-1-5-21-1757981266-507921405-1957994488-
   Queries value
1003\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
   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\ftp[use web based ftp] Oueries value: HKCU\software\microsoft\internet explorer\services[selectionactivitybuttondisable] Oueries value: $\label{lem:hkcu} \verb+KKCU\+ software \verb+\microsoft\+ internet explorer \verb+\suggested sites[enabled]+ \\$ Oueries value: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[inprocserver32] HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}\inprocserver32[] Oueries value: HKCR\clsid\{0e890f83-5f79-11d1-9043-00c04fd9189d}[appid] Oueries value: HKU\s-1-5-21-1757981266-507921405-1957994488-Oueries value: 1003\software\microsoft\windows\currentversion\internet settings\connections[defaultconnectionsettings] HKU\s-1-5-21-1757981266-507921405-1957994488-Queries value: $1003 \verb|\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]|$ HKCR\clsid\{0e890f83-5f79-11d1-9043-Queries value: 00c04fd9189d}\inprocserver32[threadingmodel] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [used omain named evolution]$ Queries value: $HKLM \verb|\system| current control set \verb|\services| tcpip \verb|\parameters| [used omain name devolution]| \\$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowungualifiedquery] Queries value: Oueries value: HKLM\svstem\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [use hosts file]$ Oueries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [registration enabled]$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: $HKLM \verb|\system| current control set \verb|\services| dns cache \verb|\parameters[register adapter name]|$ Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Queries value: Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [register wan adapters]$ Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Queries value: Oueries value $HKLM \verb|\system| current controlset \verb|\services| to pip \verb|\parameters[default registration refresh interval]| \\$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]

Queries value:

```
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
    Queries value
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
    Oueries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
    Oueries value
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]
    Queries value:
c7d49d7cecdc}[disableadapterdomainname]
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationenabled]
    Queries value:
c7d49d7cecdc}[registeradaptername]
    Queries value:
c7d49d7cecdc}[registrationmaxaddresscount]
    Queries 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:
c7d49d7cecdc}[ipautoconfigurationenabled]
    Oueries value:
c7d49d7cecdc}[addresstype]
    Queries value:
                                                       HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
    Queries value:
                                                      {\tt HKLM \coftware \ensuremath{\color{HKLM \color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\color{\ch}}}}}}}}}}}
cryptographic provider[type]
    Queries value:
                                                      HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} If the lem is a simple constant of the lem is a simple constant
cryptographic provider[image path]
    Oueries value:
                                                      HKLM\software\microsoft\cryptography[machineguid]
    Oueries value:
                                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_subdownload_lockdown[flashplayer18_a_install.exe]
    Oueries value:
                                                      HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature subdownload lockdown[*]
                                                      HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\user agent[]
                                                       HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\user agent[]
                                                      {\tt HKCU\software\microsoft\windows\currentversion\internet}
   Queries value:
settings\5.0\user agent[compatible]
                                                      HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\user agent[compatible]
   Queries value:
                                                      \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings\5.0\user agent[version]
    Queries value:
                                                      HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
   Queries value:
                                                      HKCU\software\microsoft\windows\currentversion\internet settings[user
agent]
   Oueries value:
                                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
   Oueries value:
                                                      HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
    Oueries value:
                                                      HKCU\software\microsoft\windows script\settings[jitdebug]
    Queries value:
                                                       HKCR\http\shell\open\command[]
    Queries value:
                                                      HKLM\software\microsoft\internet explorer\main[maxrenderline]
    Oueries value:
                                                      HKLM\software\microsoft\windows\currentversion\internet
settings\connections[winhttpsettings]
                                                      HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\connections[defaultconnectionsettings]
                                                      HKLM\software\microsoft\cryptography\defaults\provider types\type
    Queries value:
012[name]
   Queries value:
                                                      HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa
schannel cryptographic provider[type]
   Oueries value:
                                                      HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ microsoft \ rsa
schannel cryptographic provider[image path]
    Queries value:
                                                      HKLM\software\microsoft\cryptography\defaults\provider types\type
018[name]
    Queries value:
                                                      HKLM\software\microsoft\cryptography\defaults\provider\microsoft dh
schannel cryptographic provider[type]
    Queries value:
                                                      schannel cryptographic provider[image path]
    Queries value:
HKLM \ software \ microsoft \ cryptography \ providers \ trust \ certificate \ \{573e31f8-aaba-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-
00c04fc295ee}[$dll]
    Queries value:
```

```
HKLM\software\microsoft\cryptography\providers\trust\certificate\{573e31f8-aaba-11d0-8ccb-
00c04fc295ee}[$function]
          Oueries value:
HKLM \ software \ `microsoft\ cryptography \ providers \ 'trust\ 'final policy \ '\xi 573e 31f8-aaba-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-
00c04fc295ee}[$dl1]
          Oueries value:
HKLM\software\microsoft\cryptography\providers\trust\finalpolicy\{573e31f8-aaba-11d0-8ccb-
00c04fc295ee}[$function]
         Oueries value:
HKLM \ software \ microsoft \ cryptography \ providers \ trust \ initialization \ \{573e31f8-aaba-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8c
00c04fc295ee}[$dll]
         Queries value:
 HKLM \ software \ icrosoft \ cryptography \ providers \ trust \ initialization \ \{573e31f8-aaba-11d0-8ccb-ababa-11d0-8ccb-ababa-11d0-8ccb-ababa-ababa-11d0-8ccb-ababa-ababa-11d0-8ccb-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-ababa-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-abab-a
00c04fc295ee}[$function]
         Queries value:
                                                                                                                                        HKLM \ software \ microsoft \ cryptography \ providers \ trust \ message \ \{573e31f8-microsoft\} \ description \ 
 aaba-11d0-8ccb-00c04fc295ee}[$dll]
         Oueries value:
                                                                                                                                        aaba-11d0-8ccb-00c04fc295ee}[$function]
 00c04fc295ee}[$dl1]
          Oueries value
HKLM \ software \ microsoft \ cryptography \ providers \ trust \ signature \ \{573e31f8-aaba-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11
00c04fc295ee}[$function]
          Queries value:
HKLM \ software \ microsoft \ cryptography \ providers \ trust \ certcheck \ \{573e31f8-aaba-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11d0-8ccb-11
00c04fc295ee}[$dll]
         Queries value:
HKLM\software\microsoft\cryptography\providers\trust\certcheck\{573e31f8-aaba-11d0-8ccb-
00c04fc295ee}[$function]
                                                                                                                                       Queries value:
 aaba-11d0-8ccb-00c04fc295ee}[$dll]
         Oueries value:
                                                                                                                                        HKLM\software\microsoft\cryptography\providers\trust\cleanup\{573e31f8-
 aaba-11d0-8ccb-00c04fc295ee}[$function]
                                                                                                                                      HKLM\software\microsoft\cryptography\defaults\provider types\type
         Oueries value:
 001[name]
         Queries value:
                                                                                                                                        HKCU\software\microsoft\windows\currentversion\wintrust\trust
providers\software publishing[state]
          Oueries value:
                                                                                                                                      HKCU\software\microsoft\internet explorer\security[safety warning level]
           Queries value:
 Queries value:
 HKLM \setminus software \setminus microsoft \setminus system certificates \setminus 18f7c1fcc3090203fd5baa2f861a754976c8dd25[blob]
HKLM \label{lem:hklm} Klm \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \labe
          Queries value
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus 7f88cd7223f3c813818c994614a89c99fa3b5247[blob]
          Queries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} With the lem in the lem i
         Oueries value:
Oueries value:
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus uthroot \setminus certificates \setminus 0048f8d37b153f6ea2798c323ef4f318a5624a9e[blob]
         Oueries value:
 HKLM\software\microsoft\systemcertificates\authroot\certificates\00ea522c8a9c06aa3ecce0b4fa6cdc21d92e8099Fblobl
         Queries value:
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus uthroot \setminus certificates \setminus 0.2 faf 3 e 29 1 4 3 5 4 6 8 6 0 7 8 5 7 6 9 4 df 5 e 45 b 6 8 8 5 1 8 6 8 \lceil b \log n \rceil
         Queries value:
 Queries value:
 HKLM \setminus software \setminus microsoft \setminus system certificates \setminus authroot \setminus certificates \setminus 0.49811056 af e9f d0f 5 be 0.1685 aace 6a5 d1c4454 c [blob]
          Queries value:
 Queries value
 HKLM \setminus software \setminus microsoft \setminus system certificates \setminus authroot \setminus certificates \setminus 1331f48a5da8e01daaca1bb0c17044acfef755bb[blob]
          Queries value
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus 1f55e8839 bac \\ 30728 be \\ 7108 ede \\ 7b0 bb \\ 0d3298224 [blob]
          Oueries value
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus authroot \setminus certificates \setminus 209900b63d955728140cd13622d8c687a4eb0085[blob]
          Oueries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\216b2a29e62a00ce820146d8244141b92511b279[blob]
         Queries value
HKLM \ software \ `microsoft \ system certificates \ `authroot \ certificates \ `23e594945195f2414803b4d564d2a3a3f5d88b8c[blob]
         Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\24a40a1f573643a67f0a4b0749f6a22bf28abb6b[blob]
         Queries value:
HKLM\software\microsoft\systemcertificates\authroot\certificates\24ba6d6c8a5b5837a48db5fae919ea675c94d217[blob]
         Queries value:
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus 273ee 12457fdc 4f90c 55e8 2b56167f62f532e547[blob]
         Queries value:
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus 284f55c41a1a7a3f8328d4c262fb376ed6096f24[blob]
         Queries value:
 HKLM \setminus software \\ \setminus software 
          Oueries value:
 HKLM\software\microsoft\systemcertificates\authroot\certificates\317a2ad07f2b335ef5a1c34e4b57e8b7d8f1fca6[blob]
 HKLM \label{lem:hklm} Software \verb|\microsoft| system certificates \verb|\authroot| certificates \verb|\affine| 36863563fd5128c7bea6f005cfe9b43668086cce[blob]|
          Queries value:
 HKLM \setminus software \\ \setminus software 
          Queries value:
 Queries value:
```

 $HKLM \label{lem:hklm} KLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} which is a throat \label{lem:hklm} Label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} With \label{lem:hklm} Software \label{lem:hklm} With \label{lem:hklm}$

- HKLM\software\microsoft\systemcertificates\authroot\certificates\40e78c1d523d1cd9954fac1a1ab3bd3cbaa15bfc[blob]
 Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\43ddb1fff3b49b73831407f6bc8b975023d07c50[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\43f9b110d5bafd48225231b0d0082b372fef9a54[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\4463c531d7ccc1006794612bb656d3bf8257846f[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\47afb915cda26d82467b97fa42914468726138dd[blob]
 Oueries value:
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \mbox{\tt microsoft} \label{lem:hklm} System certificates \mbox{\tt authroot} \label{lem:hklm} Cueries \mbox{\tt value} :$
- $\label{thm:local-bound} HKLM\software\microsoft\systemcertificates\authroot\certificates\4ba7b9ddd68788e12ff852e1a024204bf286a8f6[blob] Queries value:$
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \mbox{\certificates} \label{lem:hklm} According \mbox{\certificates} \label{lem:hklm} Oueries \mbox{\certificates} \label{lem:hklm} According \mbox{\certificates} \label{lem:hklm} According \mbox{\certificates} \mbox{\certificates} \label{lem:hklm} According \mbox{\certificates} \mbox{\ce$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \system certificates \authroot \certificates \4eb6d578499b1ccf5f581ead56be3d9b6744a5e5 \[blob]\ Queries \ value:$
- $\label{thklm} \begin{tabular}{l} HKL\begin{tabular}{l} HKL\begin{tabular}{l} MKL\begin{tabular}{l} MKL\begin{tabular} MKL\begin{tabular}{l} MKL\begin{tabular}{l} MKL\begin{ta$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \system certificates \authroot \certificates \4efced 9c6bdd 0c985 ca 3c7d253063 c5be6fc620 c[blob] Queries value:$
- $\label{thm:local-bound} HKLM \software \microsoft \system certificates \authroot \certificates \4f65566336db6598581d584a596c87934d5f2ab4[blob] Queries value:$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\54f9c163759f19045121a319f64c2d0555b7e073[blob] Queries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\58119f0e128287ea50fdd987456f4f78dcfad6d4[blob] Queries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\5b4e0ec28ebd8292a51782241281ad9feedd4e4c[blob] Queries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\5e5a168867bfff00987d0b1dc2ab466c4264f956[blob] Oueries value:
- $\label{thm:local_ham} \begin{tabular}{l} HKLM \software \microsoft \system certificates \authroot \certificates \space{0.05} 5e997ca5945aab75ffd14804a974bf2ae1dfe7e1[blob] \end{tabular} Output \begin{tabular}{l} Queries \space{0.05} value: \space{0.05} \space{0.0$
- $HKLM \ software \ microsoft \ system certificates \ authroot \ certificates \ Sfb7ee 0633e259dbad0c4c9ae 6d38f1a61c7dc25[blob] \\ Queries \ value:$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\627f8d7827656399d27d7f9044c9feb3f33efa9a[blob] Queries value:
- $\label{thm:local-basis} HKLM \software \mbox{372c49}$ da9fff051b8b5c7d4e5aae30384024b9c[blob]} \\ Oueries \ value:$
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} White \labe$
- $\label{lem:hklmsoftware} HKLM \software \mbox{\sim ificates α in the continuous of the continuous o$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\687ec17e0602e3cd3f7dfbd7e28d57a0199a3f44[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\688b6eb807e8eda5c7b17c4393d0795f0fae155f[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\68ed18b309cd5291c0d3357c1d1141bf883866b1[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\69bd8cf49cd300fb592e1793ca556af3ecaa35fb[blob]
 Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\6a174570a916fbe84453eed3d070a1d8da442829[blob] Queries value:
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lklm} White \labell} White \labell{lklm} White \labell} White \labell{lklm} Whit$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\742c3192e607e424eb4549542be1bbc53e6174e2[blob]
 Queries value:

 HKLM\software\microsoft\systemcertificates\authroot\certificates\7620e71947o151b5e7o201e758fbf13aba309f7a[blob]
- $\label{thm:local-basis} HKLM \software \microsoft \system certificates \authroot \certificates \7639c71847e151b5c7ea01c758fbf12aba298f7a[blob] Queries value:$
- $\label{thm:local-bound} HKLM \software \microsoft \system certificates \authroot \certificates \auth$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \system certificates \authroot \certificates \aut$
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} White \label{lem:hklm} HKLM \label{lem:hklm} Significant \label{lem:hklm} White \label{lklm} White \label{lklm} White \label{lklm} White \label{lklm} White \label$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \system certificates \authroot \certificates \aut$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \system certificates \authroot \certificates \aut$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \system certificates \authroot \certificates \81968b3aef1cdc \colongraph \colongraph \colongraph \system \certificates \81968b3aef1cdc \colongraph \colongrap$
- $\label{thm:local-continuous} HKLM \software \microsoft \system certificates \authroot \certificates \838e30f77fdd14aa385ed145009c0e2236494faa[blob] \ Queries \ value: \\ HKLM \software \microsoft \system certificates \authroot \certificates \85371ca6e550143dce2803471bde3a09e8f8770f[blob] \\ HKLM \software \microsoft \system \certificates \authroot \certificates \85371ca6e550143dce2803471bde3a09e8f8770f[blob] \\ HKLM \software \microsoft \system \certificates \authroot \certificates \85371ca6e550143dce2803471bde3a09e8f8770f[blob] \\ HKLM \software \microsoft \system \certificates \authroot \system \cer$
- Queries value: HKLM\software\microsoft\systemcertificates\authroot\certificates\85a408c09c193e5d51587dcdd61330fd8cde37bf[blob]
- Queries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\879f4bee05df98583be360d633e70d3ffe9871af[blob] Queries value:
- $\label{thklm} \begin{tabular}{l} HKLM \software \microsoft \system certificates \authroot \certificates \8eb03fc3cf7bb292866268b751223db5103405cb[blob] \end{tabular}$ Queries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\9078c5a28f9a4325c2a7c73813cdfe13c20f934e[blob] Queries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\90aea26985ff14804c434952ece9608477af556f[blob] Queries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\90dede9e4c4e9f6fd88617579dd391bc65a68964[blob] Oueries value:

- HKLM\software\microsoft\systemcertificates\authroot\certificates\97817950d81c9670cc34d809cf794431367ef474[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\97e2e99636a547554f838fba38b82e74f89a830a[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\99a69be61afe886b4d2b82007cb854fc317e1539[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\9bacf3b664eac5a17bed08437c72e4acda12f7e7[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\9e6ceb179185a29ec6060ca53e1974af94af59d4[blob]
 Oueries value:
- $\label{thm:local-bound} HKLM \software \mbox{\tt microsoft} system certificates \authroot \certificates \9fc796e8f8524f863ae1496d381242105f1b78f5[blob] \\ Oueries \value:$
- $\label{thm:local-bound} HKLM \software \microsoft \system certificates \authroot \certificates \a399f76f0cbf4c9da55e4ac24e8960984b2905b6[blob] Queries value:$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \system certificates \authroot \certificates \as 5ec73d48c34fcbef1005aeb85843524bbfab727[blob] Queries value:$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\ab48f333db04abb9c072da5b0cc1d057f0369b46[blob]
 Queries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\aced5f6553fd25ce015f1f7a483b6a749f6178c6[blob] Queries value:
- $HKLM \ software \ microsoft \ system certificates \ b172b1a56d95f91fe50287e14d37ea6a4463768a[blob] \\ Queries \ value:$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\b19dd096dcd4e3e0fd676885505a672c438d4e9c[blob]
 Queries value:
 HKLM\software\microsoft\systemcertificates\authroot\certificates\b3eac44776c9c81ceaf29d95b6cca0081b67ec9d[blob]
- Queries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\b5d303bf8682e152919d83f184ed05f1dce5370c[blob] Queries value:
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \mbox{\certificates} \label{lem:hklm} According to the lemma \mbox{\certificates} \label{lem:hklm} We are in the lemma \mbox{\certificates} \label{lemma} We are in the lemma \mbox{\certificates} \label{lem:hklm} We are in the lem$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\b72fff92d2ce43de0a8d4c548c503726a81e2b93[blob] Oueries value:
- $\label{thm:local_ham} \begin{tabular}{l} HKLM \software \microsoft \system certificates \authroot \certificates \begin{tabular}{l} blob] \end{tabular} Queries value: \end{tabular}$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\cabb51672400588e6419f1d40878d0403aa20264[blob] Queries value:
- $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lklm} White \label{lklm} White \label{lklm} White \label{lklm} White \label{lkl$
- $\label{thm:local-bound} HKLM \software \mbox{\tt wicrosoft} system certificates \authroot \certificates \cff360f524cb20f1fead89006f7f586a285b2d5b[blob] Queries value:$
- $\label{thm:local-blob} HKLM \software \mbox{\tt microsoft} system certificates \authroot \certificates \cff810fb2c4ffc0156bfe1e1fabcb418c68d31c5[blob] Queries value:$
- $\label{thm:local-bound} HKLM \software \microsoft \system certificates \authroot \certificates \d23209 ad 23d 314232174e 40d 7f 9d 62139786633a \[blob]\ Queries \ value:$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\d29f6c98befc6d986521543ee8be56cebc288cf3[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\d2edf88b41b6fe01461d6e2834ec7c8f6c77721e[blob] Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\d4de20d05e66fc53fe1a50882c78db2852cae474[blob]
 Oueries value:
- HKLM\software\microsoft\systemcertificates\authroot\certificates\da40188b9189a3edeeaeda97fe2f9df5b7d18a41[blob] Queries value:
- $HKLM \ software \ microsoft \ system certificates \ de 28f4a4ffe 5b92fa 3c503d1a 349a7f9962a 8212[blob] \\ Queries \ value:$
- $\label{thm:local-basis} HKLM \software \microsoft \system certificates \authroot \certificates \e12dfb4b41d7d9c32b30514bac1d81d8385e2d46 \certificates \authroot \certificates \e12dfb4b41d7d9c32b30514bac1d81d8385e2d46 \certificates \end{tikzpicture} Queries value:$
- $\label{thm:local-basis} HKLM \software \microsoft \system certificates \authroot \certificates \earses \added \certificates \added \c$
- $\label{thm:local-bound} HKLM \software \microsoft \system certificates \authroot \certificates \end{time} 48e[blob] Queries value:$
- $\label{lem:hklmsoftware} HKLM \software \microsoft \system certificates \authroot \certificates \ebbc0e2d020ca69b222c2bffd203cb8bf5a82766[blob] Queries value:$
- $\label{thm:local-condition} HKLM \software \microsoft \system certificates \authroot \certificates \ecoc3716ea 9ed fadd 35d fbd 55608e60a 05d 3cb f3 [blob] Queries value:$
- HKLM\software\microsoft\systemcertificates\authroot\certificates\ef2daccbeabb682d32ce4abd6cb90025236c07bc[blob]
 Queries value:
 HKLM\software\microsoft\systemcertificates\authroot\certificates\f44095c238ac73fc4f77bf8f98df70f8f091bc52[blob]
- Queries value: HKLM\software\microsoft\systemcertificates\authroot\certificates\f88015d3f98479e1da553d24fd42ba3f43886aef[blob]
- HKLM\software\microsoft\systemcertificates\autnroot\certificates\1880f5031984/9e10a5530241042ba3143886aef[bloo Queries value: HKLM\software\microsoft\systemcertificates\ca\certificates\063da67748f0eccc690d319bcdcd0e72ac8d48d5[blob]
- Queries value:

 HKLM\software\microsoft\systemcertificates\ca\certificates\109f1caed645bb78b3ea2b94c0697c740733031c[blob]
- Queries value: HKLM\software\microsoft\systemcertificates\ca\certificates\12519ae9cd777a560184f1fbd54215222e95e71f[blob]
- $Queries\ value: \\ HKLM\ software\ microsoft\ system certificates\ value \ va$
- RKLM\software\microsoft\systemcertificates\ca\certificates\2d69a20ec4f0cd19037fd6d6246b1ee0ec41ba22[blob]
- Queries value: HKLM\software\microsoft\systemcertificates\ca\certificates\7b02312bacc59ec388feae12fd277f6a9fb4fac1[blob]
- HKLM\SoftWare\microsoft\systemcertificates\ca\certificates\/bu2312bacc59ec388feae12fd2//fba9fb4fac1[blob Queries value:
- HKLM\software\microsoft\systemcertificates\ca\certificates\8b24cd8d8b58c6da72ace097c7b1e3cea4dc3dc6[blob] Queries value:
- $\label{thm:local} HKLM \software \microsoft \system certificates \ca\certificates \9f025d9f58711a605eb0694b0e8bc0ca4f25fd6f[blob] Queries value:$

```
HKLM \backslash software \backslash microsoft \backslash system certificates \backslash ba9e3c32562a67128caabd4ab0c500bee1d0c256[blob]
    Oueries value
HKLM \label{lem:hklm} Software \verb|\microsoft| system certificates \verb|\cates| 15d3460c2c20bbe2d9fe5fb665daa2c0e225c[blob]| and the lemma system certificates \verb|\cates| 15d3460c2c20bbe2d9fe5fb665daa2c0e25c[blob]| and the lemma system certificates \verb|\cates| 15d3460c2c2c20bbe2d9fe5fb665daa2c0e25c[blob]| and the lemma system certificates 
    Oueries value:
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus f6357239b7c39725bd8000646e4a0d18ebce4cfa[blob]
    Oueries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\fe622ea7b33ca46519ab39736a66b8f6e41ff157[blob]
    Oueries value:
HKLM\software\microsoft\systemcertificates\ca\certificates\fee449ee0e3965a5246f000e87fde2a065fd89d4[blob]
    Oueries value:
HKLM\software\microsoft\systemcertificates\ca\crls\a377d1b1c0538833035211f4083d00fecc414dab[blob]
    Queries value:
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus disallowed \setminus certificates \setminus 637162 cc59a3a1e25956fa5fa8f60d2e1c52eac6[blob]
    Oueries value:
Queries value:
                                                               HKCU\software\microsoft\windows
nt\currentversion\winlogon[parseautoexec]
HKLM \setminus software \setminus microsoft \setminus system certificates \setminus authroot \setminus certificates [5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25]
    Queries value:
                                                               HKCU\software\microsoft\windows\currentversion\internet
 settings\zones\0[1c00]
    Oueries value:
                                                              \label{lem:hamiltonian} \mbox{HKLM\software\mbox{\sc microsoft\internet explorer\default behaviors[homepage]}} \mbox{\sc microsoft\sc mepage]} \mbox{\sc mic
    Queries value:
                                                              HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[inprocserver32]
    Queries value:
                                                              HKCR \verb|\clsid|{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} \verb|\inprocserver32[]|
    Oueries value:
                                                              HKCR \clsid \ \{3050f4cf-98b5-11cf-bb82-00aa00bdce0b\} [appid]
    Queries value:
                                                              HKCR\clsid\{3050f4cf-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32[threadingmodel]
                                                              HKCR\typelib\{7e8bc440-aeff-11d1-89c2-00c04fb6bfc4}\1.0\0\win32[]
    Queries value:
                                                              HKLM\software\policies\microsoft\internet explorer\main[start page]
    Oueries value:
                                                               HKCU\software\microsoft\internet explorer\main[start page]
    Queries value:
                                                              HKLM\software\microsoft\internet explorer\default behaviors[clientcaps]
    Queries value:
    Oueries value:
                                                               HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
                                                               HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
 settings[proxyoverride]
    Queries value:
                                                              HKCU\software\microsoft\windows\currentversion\internet
 settings\connections[savedlegacysettings]
    Oueries value:
                                                              HKLM\software\microsoft\internet
 explorer\main\featurecontrol\feature_maxconnectionsperserver[flashplayer18_a_install.exe]
    Queries value:
                                                              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature maxconnectionsperserver[*]
    Queries value:
                                                              HKLM\software\microsoft\internet
 explorer \verb|\main\featurecontrol\feature_maxconnectionsper1_0 server[flashplayer18_a\_install.exe]|
    Queries value:
                                                              HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_max connection sper1\_0 server[*]
    Queries value:
                                                              \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+ \\
settings[securityidiuricachesize]
    Oueries value:
                                                              HKLM\software\microsoft\windows\currentversion\internet
 settings[securityidiuricachesize]
    Oueries value:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
                                                              HKCU\software\microsoft\internet explorer\recovery[autorecover]
    Oueries value:
                                                              HKCR\.png[content type]
    Oueries value:
                                                              HKCR\clsid\{30c3b080-30fb-11d0-b724-
    Oueries value:
00aa006c1a01}\inprocserver32[inprocserver32]
                                                              HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[]
    Queries value:
                                                              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]
                                                              HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[]
    Queries value:
                                                              HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid]
     Queries value:
                                                              HKCR\clsid\{6a01fda0-30df-11d0-b724-
    Queries value:
00aa006c1a01}\inprocserver32[threadingmodel]
    Queries value:
                                                              HKCR\mime\database\content type\image/bmp\bits[0]
    Oueries value:
                                                              HKCR\mime\database\content type\image/gif\bits[0]
    Oueries value:
                                                              HKCR\mime\database\content type\image/jpeg\bits[0]
    Oueries value:
                                                              HKCR\mbox{\tt Mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt type} \mbox{\tt bits} \mbox{\tt [0]}
    Oueries value:
                                                               HKCR\mime\database\content type\image/png\bits[0]
    Oueries value:
                                                              HKCR\mbox{\tt Mime} \mbox{\tt database} \mbox{\tt content type} \mbox{\tt type} \mbox{\tt image} \mbox{\tt x-png} \mbox{\tt bits} \mbox{\tt [0]}
    Queries value:
                                                               HKCR\mime\database\content type\image/x-wmf\bits[0]
    Queries value:
                                                              \label{local-content} $HKCR\times \sigma_{\alpha}=\frac{1}{2} . $HKCR\times \sigma_{\alpha}=\frac{1}{2} 
                                                              HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
    Oueries value:
00a0c913f750}\inprocserver32[inprocserver32]
                                                              HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[]
    Queries value:
                                                              HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid]
    Queries value:
                                                              HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-
    Queries value:
 00a0c913f750}\inprocserver32[threadingmodel]
    Queries value:
                                                              HKLM\software\microsoft\cryptography\defaults\provider types\type
 024[name]
    Oueries value:
                                                              enhanced rsa and aes cryptographic provider (prototype)[type]
    Queries value:
                                                              HKLM\software\microsoft\cryptography\defaults\provider\microsoft
enhanced rsa and aes cryptographic provider (prototype)[image path]
                                                              HKCU\software\microsoft\internet
    Queries value:
 explorer\ietld\lowmic[ietlddllversionlow]
                                                              HKCU\software\microsoft\internet
    Queries value
explorer\ietld\lowmic[ietlddllversionhigh]
    Queries value:
                                                              HKCU\software\microsoft\windows\currentversion\internet
 settings\zones\3[{a8a88c49-5eb2-4990-a1a2-0876022c854f}]
    Oueries value:
                                                              HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
```

```
settings\zones\3[1a00]
   Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[160a]
   Oueries value:
                                              HKI M\software\microsoft\windows\currentversion\internet
settings\zones\0[160a]
                                              HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
   Sets/Creates value:
1.00[displayname]
   Sets/Creates value:
                                              HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[displayversion]
   Sets/Creates value:
                                              HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[versionmajor]
   Sets/Creates value:
                                              HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[versionminor]
   Sets/Creates value:
                                              1.00[publisher]
   Sets/Creates value:
                                              HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus new product
1.00[displayicon]
   Sets/Creates value:
                                              HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[uninstallstring]
                                              HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus uninstall \setminus new product
   Sets/Creates value:
1.00[urlinfoabout]
   Sets/Creates value:
                                              HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[helplink]
   Sets/Creates value:
                                              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\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[language]
   Sets/Creates value:
                                              HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
1.00[estimatedsize]
   Sets/Creates value:
                                              HKLM\software\microsoft\windows\currentversion\uninstall\newproduct
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 \setminus software \setminus microsoft \setminus windows \setminus shell no roam \setminus muicache[c: \setminus program] = (a.b., b. a.b., b. 
files\install.exe
   Sets/Creates value:
Sets/Creates value:
                                              HKLM\system\currentcontrolset\services\devicesync[description]
   Value changes:
                                              HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:
806d6172696f}[baseclass]
   Value changes:
                                              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[personal]
   Value changes:
                                              HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common documents]
                                              HKCU\software\microsoft\windows\currentversion\explorer\shell
   Value changes:
folders[desktop]
                                              HKLM\software\microsoft\windows\currentversion\explorer\shell
   Value changes:
folders[common desktop]
   Value changes:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
                                              HKCU\software\microsoft\windows\currentversion\internet
   Value changes:
settings\zonemap[intranetname]
   Value changes:
                                              \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\zonemap[uncasintranet]
                                              HKCU\software\microsoft\windows\currentversion\internet
   Value changes:
settings\zonemap[autodetect]
   Value changes:
                                              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Value changes:
                                              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
   Value changes:
                                              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[local appdata]
   Value changes:
                                              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[history]
   Value changes:
                                              HKLM\system\currentcontrolset\services\devicesync[type]
   Value changes:
                                              HKLM\software\microsoft\directdraw\mostrecentapplication[name]
                                              HKLM\software\microsoft\directdraw\mostrecentapplication[id]
   Value changes:
                                              HKU\s-1-5-21-1757981266-507921405-1957994488-
   Value changes:
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]
                                              HKU\s-1-5-21-1757981266-507921405-1957994488-
   Value changes:
1003\software\microsoft\windows\currentversion\explorer\shell folders[history]
   Value changes:
                                              HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common appdata]
                                              HKU\s-1-5-21-1757981266-507921405-1957994488-
   Value changes:
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]
                                              HKU\s-1-5-21-1757981266-507921405-1957994488-
   Value changes:
1003 \land software \land microsoft \land windows \land current version \land internet settings \land connections [savedlegacy settings]
   Value changes:
HKLM\software\microsoft\systemcertificates\authroot\certificates\5fb7ee0633e259dbad0c4c9ae6d38f1a61c7dc25[blob]
   Value changes:
                                              \label{local-constraint} \mbox{HKCU\software\mbox{\sc urrentversion\explorer\shell}} \mbox{\sc urrentversion\explorer\shell} \mbox{\sc urrentversion\explorer\shell}
```

HKCU\software\microsoft\windows\currentversion\internet

Oueries value:

folders[appdata]

Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[proxyenable]
Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings]