Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 139, Task ID: 555

Task ID: 555 Risk Level:

Date Processed: 2016-04-28 13:02:05 (UTC)

Processing Time: 62.13 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\3c8f7cba29f3aa462740dd7998c5cb74.exe"

Sample ID: 139 Type: basic admin Owner:

3c8f7cba29f3aa462740dd7998c5cb74 Label:

2016-04-28 12:45:04 (UTC) Date Added: PE32:win32:gui File Type:

File Size: 673560 bytes

3c8f7cba29f3aa462740dd7998c5cb74 MD5:

a5d8ce156441214f92d2ef6aaf78749fb7e85d6209a1d947e9675d4385a885b4 SHA256:

Description: None

Pattern Matching Results

3 Writes to a log file [Info]

- 4 Downloads executable
- 3 Long sleep detected
- 5 Creates shortcut on desktop
- 3 HTTP connection response code 200 (success) [HTTP, POST, GET, web, network, response code]

3 Creates a file extension shortcut

Static Events

Anomaly: PF: Contains a virtual section

Process/Thread Events

C:\WINDOWS\Temp\3c8f7cba29f3aa462740dd7998c5cb74.exe Creates process:

["c:\windows\temp\3c8f7cba29f3aa462740dd7998c5cb74.exe"]

Creates process: C:\WINDOWS\Temp\3c8f7cba29f3aa462740dd7998c5cb74.exe ["c:\windows\temp\3c8f7cba29f3aa462740dd7998c5cb74.exe" /_ShowProgress] Loads service: RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs] Terminates process: C:\WINDOWS\Temp\3c8f7cba29f3aa462740dd7998c5cb74.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 event:

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

507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

\BaseNamedObjects\ZonesCounterMutex Creates mutex:

\BaseNamedObjects\ZoneAttributeCacheCounterMutex Creates mutex: Creates mutex: \BaseNamedObjects\ZonesCacheCounterMutex \BaseNamedObjects\ZonesLockedCacheCounterMutex Creates mutex: Creates mutex: \BaseNamedObjects\!PrivacIE!SharedMemory!Mutex

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

settings!temporary internet files!content.ie5!

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

settings!history!history.ie5!

Creates mutex: \BaseNamedObjects\MSIMGSIZECacheMutex Creates mutex: \BaseNamedObjects\WininetConnectionMutex Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.MDH

\BaseNamedObjects\userenv: User Profile setup event Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

\BaseNamedObjects\1VtP0S1F102ZtG0W1T1C1PtP1V Creates semaphore:

Creates semaphore: \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57} \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D} Creates semaphore:

File System Events

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\00A648DE.log Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630 C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css Creates:

Creates C:\Documents and Settings\Admin\Local

```
Settings\Temp\ish10897630\css\ie6_main.css
                          C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10897630\css\main.css
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Creates:
ui
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\browse.css
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Creates:
ui\button.css
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\checkbox.css
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\images
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Creates:
ui\images\button-bg.png
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\images\progress-bg-corner.png
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\images\progress-bg.png
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Creates:
ui\images\progress-bg2.png
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\progress-bar.css
                          C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10897630\csshover3.htc
                          C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10897630\form.bmp.Mask
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\images
 Creates:
                          C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10897630\images\BG.png
                          C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10897630\images\Close.png
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Close_Hover.png
 Creates
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Color_Button.png
                          C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10897630\images\Color_Button_Hover.png
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Grey Button.png
 Creates:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Grey_Button_Hover.png
                          C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10897630\images\Icon_Generic.png
                          C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10897630\images\Loader.gif
 Creates:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Pause_Button.png
                          C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10897630\images\Progress.png
                          C:\Documents and Settings\Admin\Local
 Creates
Settings\Temp\ish10897630\images\ProgressBar.png
 Creates:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Quick_Specs.png
                         C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10897630\images\Resume_Button.png
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\locale
 Creates:
                          C:\Documents and Settings\Admin\Local
 Creates:
Settings\Temp\ish10897630\locale\DE.locale
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\locale\EN.locale
                          \label{local Settings} C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\ish10897630\sdk
 Creates:
                          C:\Documents and Settings\Admin\Local
 Creates
Settings\Temp\ish10897630\sdk\exceptlist.txt
 Creates:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\bootstrap_34287.html
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A73EE6.log
 Creates:
 Creates:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ICReinstall_3c8f7cba29f3aa462740dd7998c5cb74.exe
                          C:\Documents and Settings\Admin\Desktop\Continue Any Video Converter
 Creates:
Installation.lnk
                          C:\Documents and Settings\Admin\Local Settings\Temp\00A7403B.log
 Creates:
 Creates:
                          C:\Documents and Settings\Admin\Local Settings\Temp\is956058749
 Creates:
                          C:\Documents and Settings\Admin\Local
Settings \verb|\Temp\| is 956058749 \verb|\10961005_Setup.EXE| \\
 Creates:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\is956058749\10961005_Setup.EXE.part
                          C:\WINDOWS\Prefetch\3C8F7CBA29F3AA462740DD7998C5C-1B690EE0.pf
 Opens:
 Opens:
                          C:\Documents and Settings\Admin
 Opens:
                          C:\WINDOWS\system32\imm32.dll
 Opens:
                          C:\WINDOWS\system32\comctl32.dll
 Opens:
                          C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                          C:\WINDOWS\system32\comctl32.dll.124.Config
```

```
C:\WINDOWS\Temp\3c8f7cba29f3aa462740dd7998c5cb74.exe
 Opens:
 Opens:
                          C:\WINDOWS\system32\shell32.dll
 Opens:
                          C:\WINDOWS\system32\SHELL32.dll.124.Manifest
                          C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                          C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
 Opens:
                          C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
 Opens:
                          C:\WINDOWS\WindowsShell.Manifest
 Opens:
                          C:\WINDOWS\WindowsShell.Config
                          C:\WINDOWS\system32\URLMON.DLL.123.Manifest
 Opens:
 Opens:
                          C:\WINDOWS\system32\URLMON.DLL.123.Config
 Opens:
                          C:\WINDOWS\system32\wininet.dll.123.Manifest
 Opens:
                          C:\WINDOWS\system32\wininet.dll.123.Config
 Opens:
                          C:\WINDOWS\system32\olepro32.dll
 Opens:
                          C:\WINDOWS\system32\rpcss.dll
 Opens:
                          C:\WINDOWS\svstem32\MSCTF.dll
 Opens:
                          C:\WINDOWS\system32\MSCTFIME.IME
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temp
                          C:\Documents and Settings\Admin\Local Settings\Temp\00A648DE.log
 Opens:
 Opens:
                          C:\WINDOWS\Temp\b736b2f4-5341-4afc-9169-adecee75f4c5
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\css\ie6_main.css
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\css\main.css
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Opens:
ui
 Opens:
                          \label{local Settings} $$C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-resp. $$
ui\browse.css
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\button.css
                           {\tt C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\ish10897630\css\sdk-local\ Settings\Temp\csp.} \\
 Opens:
ui\checkbox.css
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\images
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Opens:
ui\images\button-bg.png
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\images\progress-bg-corner.png
 Opens:
                          \label{local Settings} $$C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-resp. $$
ui\images\progress-bg.png
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Opens:
ui\images\progress-bg2.png
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Opens:
ui\progress-bar.css
 Opens:
                          \label{lem:local_Settings} C:\Documents\ and\ Settings\Admin\Local\ Settings\Temp\ish10897630
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\csshover3.htc
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\form.bmp.Mask
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\images
 Opens:
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\BG.png
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\images\Close.png
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\images\Close_Hover.png
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Color_Button.png
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings \verb|\Temp\ish10897630\images\Color\_Button\_Hover.png|
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\images\Grey_Button.png
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Grey_Button_Hover.png
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\images\Icon_Generic.png
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Loader.gif
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Pause_Button.png
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\images\Progress.png
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\ProgressBar.png
 Opens:
                          C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Quick_Specs.png
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\images\Resume_Button.png
 Opens:
                          C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\locale
                          C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\locale\DE.locale
```

```
C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\locale\EN.locale
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\sdk
 Opens:
                         C:\Documents and Settings\Admin\Local
 Opens:
Settings\Temp\ish10897630\sdk\exceptlist.txt
 Opens:
                         C:\WINDOWS\system32\iphlpapi.dll
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\mprapi.dll
 Opens:
                         C:\WINDOWS\system32\activeds.dll
 Opens:
                         C:\WINDOWS\system32\adsldpc.dll
 Opens:
                         C:\WINDOWS\system32\netapi32.dll
 Opens:
                         C:\WINDOWS\system32\atl.dll
 Opens:
                         C:\WINDOWS\system32\rtutils.dll
 Opens:
                         C:\WINDOWS\system32\samlib.dll
 Opens:
                         C:\WINDOWS\system32\setupapi.dll
 Opens:
                         C:\
 Opens:
                         C:\Program Files\Internet Explorer
 Opens:
                         C:\Program Files\Internet Explorer\iexplore.exe
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\comres.dll
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
                         C:\WINDOWS\system32\ieframe.dll
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ieframe.dll.123.Config
 Opens:
                         C:\WINDOWS\system32\en-US\ieframe.dll.mui
 Opens:
                         C:\WINDOWS\system32\sxs.dll
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
 Opens:
                         C:\Documents and Settings
 Opens:
                         C:\Documents and Settings\Admin\Local Settings
 Opens:
                         C:\WINDOWS\system32\mlang.dll
                         C:\WINDOWS\system32\MLANG.dll.123.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\MLANG.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\bootstrap_34287.html
 Opens:
                         C:\WINDOWS\system32\mshtml.dll
 Opens:
                         C:\WINDOWS\system32\msls31.dll
 Opens:
                         C:\WINDOWS\system32\psapi.dll
 Opens:
                         C:\WINDOWS\system32\jscript.dll
 Opens:
                         C:\WINDOWS\system32\winlogon.exe
 Opens:
                         C:\WINDOWS\system32\xpsp2res.dll
 Opens:
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
 Opens:
                         C:\WINDOWS\Temp
 Opens:
                         C:\WINDOWS
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\ish10897630\sdk\ui\
 Opens:
 Opens:
                         C:\DOCUME~1\Admin\LOCALS~1\Temp\ish10897630\script\
                         C:\windows\temp\3c8f7cba29f3aa462740dd7998c5cb74.exe.Manifest
 Opens:
 Opens:
                         C:\windows\temp\3c8f7cba29f3aa462740dd7998c5cb74.exe.Config
 Opens:
                         C:\WINDOWS\system32\iepeers.dll
 Opens:
                         C:\WINDOWS\system32\winspool.drv
 Opens:
                         C:\WINDOWS\system32\iepeers.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\iepeers.dll.123.Config
 Opens:
                         C:\WINDOWS\svstem32\imgutil.dll
 Opens:
                         C:\WINDOWS\system32\pngfilt.dll
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\History\History.IE5
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
                         C:\Documents and Settings\Admin\Cookies
 Opens:
                         {\tt C:\Documents\ and\ Settings\Admin\Cookies\index.dat}\\
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
                         C:\WINDOWS\Fonts\arialbd.ttf
 Opens:
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
                         C:\WINDOWS\system32\powrprof.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\rasapi32.dll
 Opens:
                         C:\WINDOWS\system32\rasman.dll
 Opens:
                         C:\WINDOWS\system32\tapi32.dll
 Opens:
                         C:\WINDOWS\system32\winmm.dll
                         C:\WINDOWS\system32\TAPI32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\TAPI32.dll.124.Config
 Opens:
                         C:\AUTOEXEC.BAT
 Opens:
                         C:\Documents and Settings\All Users\Application
{\tt Data\Microsoft\Network\Connections\Pbk}
 Opens:
                         C:\WINDOWS\system32\ras
                         C:\Documents and Settings\Admin\Application
 Opens:
```

Data\Microsoft\Network\Connections\Pbk\

```
C:\WINDOWS\system32\sensapi.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
                         C:\WINDOWS\system32\rasadhlp.dll
 Opens:
                         C:\WINDOWS\system32\dnsapi.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A73EE6.log
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ICReinstall_3c8f7cba29f3aa462740dd7998c5cb74.exe
                         C:\WINDOWS\system32\drivers\etc\hosts
 Opens:
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS\system32\msv1_0.dll
                         C:\Documents and Settings\Admin\My Documents\desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\All Users
 Opens:
                         C:\Documents and Settings\All Users\Documents\desktop.ini
 Opens:
                         C:\WINDOWS\svstem32\linkinfo.dll
 Opens:
                         C:\WINDOWS\system32\ntshrui.dll
 Opens:
                         C:\WINDOWS\system32\ntshrui.dll.123.Manifest
 Opens:
                         C:\WINDOWS\system32\ntshrui.dll.123.Config
 Opens:
                         C:\Documents and Settings\Admin\Desktop
 Opens:
                         C:\Documents and Settings\Admin\Start Menu\desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\Start Menu\desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\Application Data\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\Application Data\desktop.ini
 Opens:
                         C:\Documents and Settings\Admin\My Documents
 Opens:
                         C:\Documents and Settings\Admin\My Documents\My Pictures\Desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\Documents
                         C:\Documents and Settings\All Users\Documents\My Pictures\Desktop.ini
 Opens:
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Music\Desktop.ini
 Opens:
                         C:\Documents and Settings\All Users\Documents\My Videos\Desktop.ini
 Opens:
                         C:\WINDOWS\system32\msimg32.dll
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A7403B.log
 Opens:
                         C:\Documents and Settings\Admin\Local Settings\Temp\is956058749
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\is956058749\10961005_Setup.EXE
 Opens:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\is956058749\10961005_Setup.EXE.part
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A648DE.log
 Writes to:
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings \verb|\Temp\ish10897630\css\ie6_main.css| \\
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\css\main.css
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Writes to:
ui\browse.css
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\button.css
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\checkbox.css
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\images\button-bg.png
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Writes to:
ui\images\progress-bg-corner.png
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\images\progress-bg.png
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
ui\images\progress-bg2.png
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Writes to:
ui\progress-bar.css
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\ish10897630\csshover3.htc
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\form.bmp.Mask
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\ish10897630\images\BG.png
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Close.png
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Close_Hover.png
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\ish10897630\images\Color_Button.png
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Color_Button_Hover.png
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Grey_Button.png
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Grey_Button_Hover.png
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Icon_Generic.png
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Loader.gif
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\ish10897630\images\Pause_Button.png
```

```
Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Progress.png
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\ProgressBar.png
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\ish10897630\images\Quick_Specs.png
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Resume_Button.png
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\locale\DE.locale
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\ish10897630\locale\EN.locale
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\sdk\exceptlist.txt
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\bootstrap_34287.html
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A73EE6.log
 Writes to:
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ICReinstall_3c8f7cba29f3aa462740dd7998c5cb74.exe
                         C:\Documents and Settings\Admin\Desktop\Continue Any Video Converter
 Writes to:
Installation.lnk
 Writes to:
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A7403B.log
 Writes to:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\is956058749\10961005_Setup.EXE
                         C:\Documents and Settings\Admin\Local
 Writes to:
Settings\Temp\is956058749\10961005_Setup.EXE.part
                         C:\WINDOWS\Temp\3c8f7cba29f3aa462740dd7998c5cb74.exe
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A648DE.log
 Reads from:
                         C:\WINDOWS\Registration\R00000000007.clb
 Reads from:
                         C:\WINDOWS\system32\ieframe.dll
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\bootstrap_34287.html
                         C:\Documents and Settings\Admin\Local Settings\Temp\ish10897630\css\sdk-
 Reads from:
ui\progress-bar.css
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\css\main.css
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10897630\images\BG.png
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Quick_Specs.png
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\locale\EN.locale
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10897630\images\Grey_Button.png
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Color_Button.png
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Close.png
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10897630\images\Loader.gif
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10897630\images\ProgressBar.png
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Progress.png
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10897630\images\Pause_Button.png
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Resume_Button.png
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10897630\form.bmp.Mask
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Close_Hover.png
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ish10897630\images\Grey_Button_Hover.png
                         C:\Documents and Settings\Admin\Local
 Reads from:
Settings\Temp\ish10897630\images\Color_Button_Hover.png
 Reads from:
                         C:\AUTOEXEC.BAT
                         C:\Documents and Settings\Admin\Local Settings\Temp\00A73EE6.log
 Reads from:
                         C:\Documents and Settings\Admin\Local
Settings\Temp\ICReinstall_3c8f7cba29f3aa462740dd7998c5cb74.exe
 Reads from:
                         C:\WINDOWS\system32\drivers\etc\hosts
 Reads from:
                         C:\WINDOWS\system32\rsaenh.dll
 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:\Documents and Settings\Admin\Start Menu\desktop.ini
                         C:\Documents and Settings\All Users\Start Menu\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\All Users\Application Data\desktop.ini
                         C:\Documents and Settings\Admin\Application Data\desktop.ini
 Reads from:
 Reads from:
                         C:\Documents and Settings\Admin\My Documents\My Pictures\Desktop.ini
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Pictures\Desktop.ini
 Reads from:
                         C:\Documents and Settings\All Users\Documents\My Music\Desktop.ini
                         C:\Documents and Settings\All Users\Documents\My Videos\Desktop.ini
 Reads from:
```

C:\Documents and Settings\Admin\Local

Reads from:

Settings\Temp\ish10897630\images\Icon_Generic.png

C:\Documents and Settings\Admin\Local Settings\Temp\00A7403B.log Reads from: Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\00A648DE.log

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

Settings\Temp\ish10897630\bootstrap_34287.html

Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\00A73EE6.log C:\Documents and Settings\Admin\Local Settings\Temp\00A7403B.log Deletes:

Network Events

DNS query: os.softwarenetcdn.com DNS auery: www.soft-ware.net DNS query: az745193.vo.msecnd.net

os.softwarenetcdn.com \Rightarrow 52.49.88.152 DNS response: DNS response: os.softwarenetcdn.com \Rightarrow 52.18.52.15 os.softwarenetcdn.com ⇒ 54.229.179.58 DNS response: DNS response: www.soft-ware.net \Rightarrow 104.27.165.7 DNS response: www.soft-ware.net \Rightarrow 104.27.164.7 DNS response: cs3.wpc.v0cdn.net \Rightarrow 68.232.45.201

52.49.88.152:80 Connects to: Connects to: 104.27.165.7:80 Connects to: 68.232.45.201:80 Sends data to: 8.8.8.8:53

www.soft-ware.net:80 (104.27.165.7) Sends data to: Sends data to: os.softwarenetcdn.com:80 (52.49.88.152) Sends data to: cs3.wpc.v0cdn.net:80 (68.232.45.201) Receives data from: 0.0.0.0:0

os.softwarenetcdn.com:80 (52.49.88.152) Receives data from: Receives data from: www.soft-ware.net:80 (104.27.165.7) Receives data from: cs3.wpc.v0cdn.net:80 (68.232.45.201)

Windows Registry Events

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

Creates key:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints \\ 2 \setminus \{f90255c2-6bc4-11e3-9fc7-12e3-12e4\} \setminus factor \\ 2 \setminus \{f90255c2-6bc4-11e3-9fc7-12e4\} \setminus factor \\ 3 \setminus \{f90255c2-6bc4-11e3-9fc7-12e4\} \setminus factor \\ 4 \setminus \{f9025c2-6bc4-11e3-9fc7-12e4\} \setminus factor \\ 4 \setminus \{f9025c2-6bc4-12e4\} \setminus factor \\ 4 \setminus \{f9025c2-6bc4-12e4\} \setminus factor \\ 4 \setminus \{f9025c2-6bc4-12e4\} \setminus factor \\ 4 \setminus \{f9025c2$

806d6172696f}\

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

folders

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

Creates key: HKLM\software\microsoft\tracing

Creates key: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} soft \label{thm:local_hammon} with the label{thm:local_hammon} \end{tabular} \begin{tabular}{ll} HKLM \label{thm:local_hammon} soft \label{thm:local_hammon} \end{tabular} \begi$

folders

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

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

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

settings\connections

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

awareness Creates kev:

HKLM\system\currentcontrolset\services\tcpip\parameters Deletes value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

options\3c8f7cba29f3aa462740dd7998c5cb74.exe

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

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

options\gdi32.dll

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

options\user32.dll

Opens kev: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\system\currentcontrolset\control\safeboot\option

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

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

options\imm32.dll

Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll

Opens key: options\secur32.dll

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

options\rpcrt4.dll

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

options\advapi32.dll Opens key:

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

options\ole32.dll

Opens key:

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

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

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

options\oleaut32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\comctl32.dll Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre_initialize$ Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\windows Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon HKLM\ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics Opens key: HKLM\software\microsoft\ole Opens key: HKCR\interface HKCR\interface\{00020400-0000-0000-c000-00000000046} Opens key: Opens key: HKLM\software\microsoft\oleaut HKLM\software\microsoft\oleaut\userera Opens kev: Opens key: HKCU\ Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens key: HKCU\control panel\desktop Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll Opens kev: HKLM\software\microsoft\windows\currentversion\explorer\performance Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll HKLM\system\setup Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comdlg32.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\iertutil.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\urlmon.dll Opens key: HKCU\software\classes\ HKCU\software\classes\protocols\name-space handler\ Opens key: Opens key: HKCR\protocols\name-space handler Opens key: HKCU\software\classes\protocols\name-space handler Opens key: $\label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\internet}} \\$ settings HKLM\software\microsoft\windows\currentversion\internet settings Opens kev: Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature protocol lockdown HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\ Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol HKLM\software\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol Opens kev: 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 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}$ settings\zonemap\domains\ HKLM\software\policies\microsoft\windows\currentversion\internet Opens kev: settings\zonemap\ranges\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\ Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck HKLM\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_unc_savedfilecheck

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

options\version.dll

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

options\normaliz.dll

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

options\wininet.dll

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

Opens key: HKCU\software\borland\locales
Opens key: HKLM\software\borland\locales
Opens key: HKCU\software\borland\delphi\locales

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

options\olepro32.dll

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

options\msctf.dll

Opens key:

HKLM\software\microsoft\ctf\compatibility\3c8f7cba29f3aa462740dd7998c5cb74.exe

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

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

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

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

options\msctfime.ime

Opens key: HKCU\software\microsoft\ctf

Opens key: ${\it HKLM \backslash software \backslash microsoft \backslash ctf \backslash systems hared}$ ${\it HKLM \ } software \ `microsoft \ 'rpc \ 'paged buffers$ Opens key:

Opens key: HKLM\software\microsoft\rpc

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

options\3c8f7cba29f3aa462740dd7998c5cb74.exe\rpcthreadpoolthrottle Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\control\computername

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

options\ws2help.dll

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

options\ws2_32.dll

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

options\iphlpapi.dll

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

 $HKLM \verb|\system| current control set \verb|\services| net bt \verb|\parameters| interfaces |$ Opens key:

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

Opens key:

c7d49d7cecdc}

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

options\netapi32.dll

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

options\wldap32.dll

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

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

options\adsldpc.dll

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

options\atl.dll Opens kev:

options\activeds.dll

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

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

Opens key:

 $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ options\samlib.dll

Opens kev:

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

options\setupapi.dll

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

HKLM\system\wpa\pnp Opens key:

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

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

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters Opens key: HKLM\software\policies\microsoft\system\dnsclient

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

options\mprapi.dll

Opens key:

Opens key: $\label{lower} \verb|HKCU| software\classes \verb|http\shell| open\command | lower |$

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

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

HKLM\software\microsoft\com3 Opens key:

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

Opens key:

 $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$

options\clbcatq.dll

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

Opens key: HKLM\software\classes

Opens key: HKU\

Opens key: HKCR\clsid

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

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

00c04fd705a2}\treatas

 $HKCR \clsid \ \ \{8856f961-340a-11d0-a96b-00c04fd705a2\} \ \ treat as$ 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

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

00c04fd705a2}\inprochandler32

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

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

00c04fd705a2}\inprochandlerx86

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

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

00c04fd705a2}\localserver

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

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

options\ieframe.dll

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

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

0000c05bae0b}\typelib

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

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

00aa00404770}\proxystubclsid32

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

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

00aa004ba90b}\proxystubclsid32

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

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

00000000046}\proxystubclsid32

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

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

 $00c04f79abd1\\ \\ \ proxystubclsid32$

Opens key: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32
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\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}

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

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

Opens key: $\label{eq:hccn} \begin{tabular}{ll} HKCR \typelib & eab22ac0-30c1-11cf-a7eb-0000c05bae0b \ 1.1 \\ Opens key: & HKCU \software \classes \typelib & eab22ac0-30c1-11cf-a7eb-0000c05bae0b \ 1.2 \\ HKCU \software \classes \typelib \ 1.3 \\ HKCU \software \classes \clas$

0000c05bae0b}\1.1\0

0000c05bae0b}\1.1\0\win32

Opens key: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32

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

settings\zonemap\

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001

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

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

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

settings\zonemap\ranges\

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

settings\zonemap\protocoldefaults\

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

settings\zonemap\domains\

Opens kev:

 $Opens \ key: \\ HKLM\software\microsoft\windows\currentversion\label{eq:hklm} internet$

settings\zonemap\domains\
 Opens key: HKLM\software\microsoft\windows\currentversion\internet

settings\zonemap\domains\msn.com
 Opens key: HKLM\software\microsoft\windows\currentversion\internet

Opens key: HKLM\software\m: settings\zonemap\domains\msn.com\related

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination

Opens key: HKLM\software\microsoft\internet

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

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

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
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

HKCU\software\microsoft\windows\currentversion\internet settings\zones\4

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

```
settings\zones\
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:
                                      \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings\zones\0
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\1
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:
                                      \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zones\2
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\2
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\4
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\4
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\0
  Opens key:
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\1
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\1
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\1
                                      HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\2
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\2
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\2
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                                      HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\lockdown_zones\3
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Opens key:
                                      HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\lockdown_zones\4
  Opens key:
                                      HKCR\clsid\{3050f4e1-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                      HKCR\clsid\{3050f4f5-98b5-11cf-bb82-00aa00bdce0b}
                                      HKCR\clsid\{3050f819-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\internet settings
  Opens kev:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
                                      HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature http username password disable
  Opens key:
                                      HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                                      HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
  Opens kev:
                                      HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
                                      HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
HKLM \ software \ `microsoft \ 'windows \ 'current version' shell compatibility \ 'applications' \ '3c8f7cba29f3aa462740dd7998c5cb74. exemple the shell compatibility \ 'applications' \ 'according to the shell 
  Opens kev:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-
a2d8-08002b30309d}
                                      HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
  Opens key:
08002b30309d}\inprocserver32
  Opens key:
                                      HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
  Opens kev:
HKCU \ software \ microsoft \ windows \ current version \ \ explorer \ \ mountpoints \ 2 \ cpc \ \ \ volume
```

Opens key:

11e3-9fc7-806d6172696f}\

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

Opens key: HKCR\drive\shellex\folderextensions

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

4442-804e-409d6c4515e9}

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

409d6c4515e9}

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

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

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

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: $\label{lem:hkcusoftware} \mbox{ HKCU\software\classes\directory\shellex\label{lem:hkcusoftware} HKCU\software\classes\directory\shellex\label{lem:hkcusoftware} \mbox{ HKCU\software\classes\directory\shellex\label{lem:hkcusoftware} } \mbox{ HKCU\software\classes\directory\shellex\label{lem:hkcusoftware\classes\directory\shellex\label{lem:hkcusoftware\classes\directory\shellex\label{lem:hkcusoftware\classes\directory\shellex\labellex\labellex} \mbox{ HKCU\software\classes\directory\shellex\labellex\l$

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\clsid

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

Opens key: HKCU\software\classes\.html

Opens key: HKCR\.html

Opens key: HKCU\software\classes\htmlfile

Opens key: HKCR\htmlfile

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

Opens key: HKCR\htmlfile\curver
Opens key: HKCR\htmlfile\

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

Opens key: HKCR\htmlfile\shellex\iconhandler

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

Opens key: HKCR\systemfileassociations\.html

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

Opens key: HKCR\systemfileassociations\text
Opens key: HKCU\software\classes\htmlfile\clsid

Opens key: HKCR\htmlfile\clsid

 $Opens \; key: \\ HKCU \setminus software \land classes \land clsid \land \{25336920-03f9-11cf-8fd0-00aa00686f13\} \land categories \land \{00021490-0000-0000-c000-00000000046\} \\$

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

categories\{00021490-0000-0000-c000-00000000046}

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

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

13914bef5890}

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

13914bef5890}

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

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

6a27-4817-a6f2-13914bef5890}

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

13914bef5890}

Opens key: HKCU\software\classes*

Opens key: HKCR*

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

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_show_failed_connect_content_kb942615

Opens key: HKLM\software\microsoft\internet

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

options\mlang.dll

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

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

000000000046}

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

00000000046}

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

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

0000-0000-c000-000000000046}

```
HKCR\systemfileassociations\text\shellex\{000214e6-0000-0000-c000-
 Opens key:
000000000046}
                         HKCU\software\classes\*\shellex\{000214e6-0000-0000-c000-000000000046}
 Opens kev:
                         HKCR\*\shellex\{000214e6-0000-0000-c000-00000000046}
 Opens key:
 Opens key:
                         HKLM\software\policies\microsoft\internet explorer\browseremulation
 Opens key:
                         HKCU\software\policies\microsoft\internet explorer\browseremulation
                         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:
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
 Opens key:
                         HKCU\software\microsoft\internet explorer
 Opens key:
                         HKLM\software\microsoft\internet explorer
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
 Opens key:
                        HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
 Opens key:
                         HKCU\software\classes\protocols\name-space handler\file\
 Opens key:
                         HKCR\protocols\name-space handler\file
                         HKCU\software\classes\protocols\name-space handler\*\
 Opens kev:
 Opens key:
                         HKCR\protocols\name-space handler\*
 Opens key:
                         HKCU\software\classes\protocols\filter\text/html
 Opens key:
                         HKCR\protocols\filter\text/html
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_sniffing
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_mime_sniffing
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_safe_bindtoobject
                         HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_safe_bindtoobject
                         Opens key:
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\treatas
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\treatas
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\inprocserver32
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens kev:
00aa00686f13}\inprocserverx86
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserverx86
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver32
 Opens key:
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver32
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens kev:
00aa00686f13}\inprochandler32
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandler32
 Opens key:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
 Opens key:
00aa00686f13}\inprochandlerx86
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprochandlerx86
 Opens key:
 Opens kev:
                         HKCU\software\classes\clsid\{25336920-03f9-11cf-8fd0-
00aa00686f13}\localserver
                         HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\localserver
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
options\msls31.dll
 Opens key:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mshtml.dll
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_css_data_respects_xss_zone_setting_kb912120
                         HKLM\software\microsoft\internet
 Opens kev:
explorer\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
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_external_style_sheet_fix_for_smartnavigation_kb926131
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_aria_support
                         HKLM\software\microsoft\internet
 Opens kev:
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 kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_private_font_setting
 Opens key:
                         HKCU\software\microsoft\internet
```

explorer\main\featurecontrol\feature_css_show_hide_events

```
HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_css_show_hide_events
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
  Opens kev:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_display_node_advise_kb833311
                                    HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_expanduri_bypass
  Opens kev:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_body_size_in_editable_iframe_kb943245
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_databinding_support
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enforce_bstr
                                    HKCU\software\microsoft\internet
  Opens kev:
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
                                    HKLM\software\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_object_caching
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_legacy_tostring_in_compatview
  Opens kev:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_om_screen_origin_display_pixels
  Opens key:
                                    HKCU\software\microsoft\windows nt\currentversion\windows
  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
                                    HKCU\software\policies\microsoft\internet explorer\domstorage
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet explorer\domstorage
  Opens key:
                                    HKLM\software\microsoft\internet explorer\domstorage
                                    HKLM\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
  Opens key:
                                    HKCU\software\policies\microsoft\internet explorer\safety\privacie
  Opens key:
                                    HKCU\software\microsoft\internet explorer\safety\privacie
                                    HKLM\software\microsoft\internet explorer\safety\privacie
  Opens key:
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
                                    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
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_restrict_filedownload
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_restrict_filedownload
  Opens key:
                                    HKLM\software\microsoft\internet explorer\security\floppy access
  Opens key:
                                    HKCU\software\microsoft\internet explorer\security\adv addrbar spoof
detection
  Opens key:
                                    HKLM\software\microsoft\internet explorer\security\adv addrbar spoof
detection
  Opens key:
                                    HKCU\software\classes\protocols\name-space handler\about\
  Opens key:
                                    HKCR\protocols\name-space handler\about
                                    HKCU\software\classes\protocols\handler\about
  Opens key:
  Opens key:
                                    HKCR\protocols\handler\about
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}
  Opens key:
  Opens key:
                                    HKCU \setminus software \setminus classes \setminus clsid \setminus \{3050f406-98b5-11cf-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
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\treatas
  Opens key:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserver32
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32
  Opens kev:
  Opens key:
                                    HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-
00aa00bdce0b}\inprocserverx86
  Opens key:
                                    HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\tinprocserverx86
```

```
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}\inprochandler32

Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprochandlerx86

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\localserver

Opens key: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\localserver

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

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

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

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

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

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

00aa00686f13}\progid

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

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

explorer\main\featurecontrol\feature_legacy_dlcontrol_behaviors

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

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

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

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

 $Opens\ key: \\ HKCU \ software \ microsoft \ windows \ current version \ policies \ active desktop$

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

Opens key: HKCU\software\microsoft\internet explorer\international\scripts\3
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\travellog
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\travellog

Opens key: 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

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

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

Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\zones\0

Opens key: HKCU\software\microsoft\internet

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\policies\microsoft\windows\currentversion\internet

settings\

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

settings\zonemap\
Opens kev:

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

settings\zonemap\

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

f4ceaaf59cfc}\inprocserver32

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

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

f4ceaaf59cfc}\inprocserverx86

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

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

f4ceaaf59cfc}\localserver32

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

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

f4ceaaf59cfc}\inprochandler32

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

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

f4ceaaf59cfc}\inprochandlerx86

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

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

f4ceaaf59cfc}\localserver

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

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

options\msimtf.dll

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

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

c9633f71be64}\languageprofile

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

c9633f71be64}\languageprofile

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

c9633f71be64}\languageprofile\0x00000000

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

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

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

431b3828ba53}\treatas

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

431b3828ba53}\inprocserver32

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

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

431b3828ba53}\inprocserverx86

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

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

431b3828ba53}\localserver32

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

431b3828ba53}\inprochandler32

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

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

431b3828ba53}\inprochandlerx86

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

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

431b3828ba53}\localserver

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

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

869523e2d6c7}\treatas

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

869523e2d6c7}\inprocserver32

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

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

869523e2d6c7}\inprocserverx86

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

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

869523e2d6c7}\localserver32

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

Opens key:

869523e2d6c7}\inprochandler32

Opens key:

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

869523e2d6c7}\inprochandlerx86

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

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

869523e2d6c7}\localserver

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

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

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

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

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

Opens key: $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = \{c1ee01f2-b3b6-4a6a-9ddb-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a$

```
e988c088ec82}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
                                                                  HKLM\software\microsoft\ctf\tip\{dcbd6fa8-032f-11d3-b5b1-
    Opens key:
HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-
    Opens key:
Of816c09f4ee}\category\category\{b95f181b-ea4c-4af1-8056-7c321abbb091}
    Opens key:
                                                                  HKCU\software\microsoft\ctf\langbaraddin\
                                                                  HKLM\software\microsoft\ctf\langbaraddin\
    Opens key:
                                                                  HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
    Opens key:
c9633f71be64}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
    Opens key:
                                                                  HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
    Opens key:
                                                                  HKLM \setminus software \setminus microsoft \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = \{c1ee01f2-b3b6-4a6a-9ddb-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a
e988c088ec82}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
                                                                  Opens key:
00c04fc324a1}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
    Opens key:
                                                                  HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9ac2-4008-9a
Of816c09f4ee}\category\category\{534c48c1-0607-4098-a521-4fc899c73e90}
    Opens key:
                                                                  HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                  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
   Opens key:
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
    Opens key:
                                                                  HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
    Opens key:
                                                                  HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                  HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
   Opens key:
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
    Opens key:
                                                                  HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80\} \verb|\category\item|{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}|
    Opens key:
                                                                  HKCU\software\policies\microsoft\internet explorer\control panel
    Opens key:
                                                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
    Opens key:
                                                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_iedde_register_urlecho
                                                                  HKCU \setminus software \setminus classes \setminus clsid \setminus \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\}
    Opens key:
    Opens key:
                                                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
    Opens key:
                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\treatas
    Opens key:
                                                                  HKCR \clsid \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \treatas
    Opens key:
                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32
    Opens key:
                                                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32
    Opens key:
                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserverx86
    Opens key:
                                                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprocserverx86
    Opens key:
                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver32
    Opens key:
                                                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\localserver32
                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
    Opens kev:
00aa00bbbb58}\inprochandler32
                                                                  HKCR\clsid\f414c260-6ac0-11cf-b6d1-00aa00bbbb58\\\inprochandler32
    Opens key:
                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
    Opens key:
00aa00bbbb58}\inprochandlerx86
    Opens key:
                                                                  HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbb58}\inprochandlerx86
    Opens kev:
                                                                  HKCU\software\classes\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\localserver
                                                                  HKCR \ clsid \ \{f414c260-6ac0-11cf-b6d1-00aa00bbbb58\} \ localserver
    Opens key:
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options\jscript.dll
    Opens key:
                                                                  HKLM\software\microsoft\windows script\features
    Opens key:
                                                                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
                                                                  HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_respect_objectsafety_policy_kb905547
    Opens key:
                                                                  {\tt HKLM \setminus software \setminus microsoft \setminus internet\ explorer \setminus activex\ compatibility}
    Opens key:
                                                                  HKLM\software\microsoft\internet explorer\activex
compatibility\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}
                                                                  HKLM\system\currentcontrolset\control\nls\locale
    Opens key:
    Opens key:
                                                                  HKLM \ system \ current controls et \ control \ nls \ locale \ alternate \ sorts
    Opens key:
                                                                  HKLM\system\currentcontrolset\control\nls\language groups
                                                                  HKCU\software\classes\appid\3c8f7cba29f3aa462740dd7998c5cb74.exe
    Opens key:
    Opens key:
                                                                  HKCR\appid\3c8f7cba29f3aa462740dd7998c5cb74.exe
    Opens key:
                                                                  HKLM\system\currentcontrolset\control\lsa
    Opens key:
                                                                  HKCU\software\microsoft\windows\currentversion\internet settings\url
history
    Opens kev:
                                                                  HKCU\software\microsoft\ftp
                                                                  HKLM\software\policies\microsoft\internet explorer\services
    Opens key:
    Opens key:
                                                                  HKCU\software\microsoft\internet explorer\services
    Opens key:
                                                                  HKLM\software\microsoft\internet explorer\services
    Opens key:
                                                                  HKLM\software\policies\microsoft\internet explorer\activities
    Opens key:
                                                                  HKCU\software\microsoft\internet explorer\activities
                                                                  HKLM\software\microsoft\internet explorer\activities
    Opens kev:
```

HKLM\software\policies\microsoft\internet

Opens key:

explorer\infodelivery\restrictions

HKCU\software\policies\microsoft\internet Opens kev:

explorer\infodelivery\restrictions

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_binary_caller_service_provider

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

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_additional_ie8_memory_cleanup

HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: 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\software\microsoft\windows nt\currentversion\image file execution

options\xpsp2res.dll

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

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

HKI M\software\microsoft\windows Opens kev:

nt\currentversion\appcompatflags\custom\3c8f7cba29f3aa462740dd7998c5cb74.exe

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

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

be2efd2c1a33}

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes

Opens key:

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

edd5fbde1328} Opens key:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-4df9-a57$

b813f72dbb91} Opens kev:

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

7c29ddecae3f}

Opens key:

085bcc18a68d} Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}

Opens key:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus urlzones$

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature activex inactivate mode removal revert

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_activex_inactivate_mode_removal_revert Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths

Opens key:

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones HKCU\software\microsoft\internet Opens kev:

explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105

HKLM\software\microsoft\internet Opens kev: explorer\main\featurecontrol\feature_ignore_leading_file_separator_in_uri_kb933105

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

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus has hes$

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones

Opens kev:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths

Opens kev:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus has hes$

Opens key:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths Opens key: $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes$

```
Opens key:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \oline \oline \code identifiers \code \code \end{tabular} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code \cod
               Opens kev:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
               Opens kev:
                                                                                                                                                                                                            HKLM\software\microsoft\internet
   explorer\main\featurecontrol\feature_subdownload_lockdown
               Opens key:
```

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus has hes$ Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones

Opens kev:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \end{tabular} $$ $$ \align{tabular}{ll} Akcular \end{tabular} $$ \align{tabular}{ll} Akcular$

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones

HKCU\software\classes\.css Opens kev:

Opens key: HKCR\.css

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_custom_image_mime_types_kb910561

Opens kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones

Opens kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes

Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones

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

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

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

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation

HKLM\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_cross_domain_redirect_mitigation Opens key: HKLM\software\microsoft\internet explorer\default behaviors

 $HKCU \setminus software \setminus classes \setminus clsid \setminus \{3050f4cf-98b5-11cf-bb82-00aa00bdce0b\}$ Opens key:

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b} Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\treatas

Opens key: $HKCR\clsid$ {3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\treatas HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-Opens kev:

00aa00bdce0b}\inprocserver32

HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\inprocserverx86

Opens key: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\localserver32

HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\localserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\inprochandler32

Opens key: $\label{lem:hkcr} $HKCR\clsid{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\ender 32$$

Opens key: HKCU\software\classes\clsid\{3050f4cf-98b5-11cf-bb82-

00aa00bdce0b}\inprochandlerx86

HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}\inprochandlerx86 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\winspool.drv Opens key:

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

options\iepeers.dll

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

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_scripturl_mitigation HKCU\software\classes\.png Opens key:

Opens key:

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

options\imgutil.dll

Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{30c3b080-30fb-11d0-b724-00aa006c1a01\}$

HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01} Opens kev: Opens key: 00aa006c1a01}\treatas

HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\treatas Opens kev: Opens key: HKCU\software\classes\clsid\{30c3b080-30fb-11d0-b724-

00aa006c1a01}\inprocserver32

Opens kev: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32

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

HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver32 Opens kev:

Opens key:

00aa006c1a01}\inprochandler32

HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandler32 Opens key:

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

00aa006c1a01}\inprochandlerx86

HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprochandlerx86 Opens kev:

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

00aa006c1a01}\localserver

HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\localserver Opens key: Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}

HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01} Opens key: HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens kev:

00aa006c1a01}\treatas

Opens key: $HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01\}\treatas$ Opens key:

00aa006c1a01}\inprocserver32

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32

HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens kev:

00aa006c1a01}\inprocserverx86

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserverx86

HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens key:

00aa006c1a01}\localserver32

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver32

HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens key:

00aa006c1a01}\inprochandler32

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprochandler32

HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens key:

00aa006c1a01}\inprochandlerx86

Opens key: $HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\tinprochandlerx86$

HKCU\software\classes\clsid\{6a01fda0-30df-11d0-b724-Opens key:

00aa006c1a01}\localserver

Opens key: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\localserver

HKCU\software\classes\mime\database\content type Opens key:

Opens key: HKCR\mime\database\content type

HKCU\software\classes\mime\database\content type\image/bmp\bits Opens key:

Opens key: HKCR\mime\database\content type\image/bmp\bits

Opens key: HKCU\software\classes\mime\database\content type\image/gif\bits

Opens kev: HKCR\mime\database\content type\image/gif\bits

Opens key: HKCU\software\classes\mime\database\content type\image/jpeg\bits Opens key:

HKCR\mime\database\content type\image/jpeg\bits Opens key: HKCU\software\classes\mime\database\content type\image/pjpeg\bits

Opens key: HKCR\mime\database\content type\image/pjpeg\bits

Opens key: HKCU\software\classes\mime\database\content type\image/png\bits

Opens kev: HKCR\mime\database\content type\image/png\bits

Opens key: HKCU\software\classes\mime\database\content type\image/tiff\bits

Opens key: HKCR\mime\database\content type\image/tiff\bits

Opens key: HKCU\software\classes\mime\database\content type\image/x-icon\bits

Opens key: HKCR\mime\database\content type\image/x-icon\bits

HKCU\software\classes\mime\database\content type\image/x-jg\bits Opens key:

Opens key: HKCR\mime\database\content type\image/x-jg\bits Opens key:

HKCU\software\classes\mime\database\content type\image/x-png\bits Opens key: HKCR\mime\database\content type\image/x-png\bits

Opens key:

HKCU\software\classes\mime\database\content type\image/x-wmf\bits

Opens key: HKCR\mime\database\content type\image/x-wmf\bits HKCU\software\classes\mime\database\content type\image/x-png Opens key:

Opens key: HKCR\mime\database\content type\image/x-png

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

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

00a0c913f750}\treatas

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

00a0c913f750}\inprocserver32

Opens key: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32

HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-Opens kev:

00a0c913f750}\inprocserverx86

HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserverx86 Opens kev:

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

00a0c913f750}\localserver32

Opens key: $HKCR\clsid\\a3ccedf7-2de2-11d0-86f4-00a0c913f750\\\localserver32$

HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-Opens kev:

00a0c913f750}\inprochandler32

HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprochandler32 Opens key:

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

00a0c913f750}\inprochandlerx86

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

Opens kev: HKCU\software\classes\clsid\{a3ccedf7-2de2-11d0-86f4-

00a0c913f750}\localserver

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

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

options\pngfilt.dll

Opens key: HKCU\software\classes\.gif

HKCR\.gif Opens key:

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

settings\5.0\cache

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

settings\5.0\cache

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content

Opens key:

HKLM\software\microsoft\windows\currentversion\internet

settings\5.0\cache\content

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

settings\5.0\cache\cookies

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

settings\5.0\cache\cookies

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

settings\5.0\cache\history

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

settings\5.0\cache\history

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

settings\5.0\cache\extensible cache

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

settings\5.0\cache\extensible cache\domstore

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

settings\5.0\cache\extensible cache\feedplat

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

settings\5.0\cache\extensible cache\iecompat

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

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

settings\5.0\cache\extensible cache\mshist012014041220140413

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

settings\5.0\cache\extensible cache\privacie:

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

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

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

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

Opens key: $HKLM \setminus software \setminus microsoft \setminus tip \setminus \{c1ee01f2-b3b6-4a6a-9ddd-based \} = \{c1ee01f2-b3b6-4a6a-9ddb-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a6a-9db-based \} = \{c1ee01f2-b3b6-4a$

e988c088ec82}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}

Opens key: $HKLM \setminus software \setminus icrosoft \setminus tip \setminus \{dcbd6fa8-032f-11d3-b5b1-143-$

00c04fc324a1}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}

HKLM\software\microsoft\ctf\tip\{f89e9e58-bd2f-4008-9ac2-Opens kev:

Of816cO9f4ee}\category\item\{a48fa74e-f767-44e4-bfbc-169e8b38ff58}

HKCU\software\microsoft\internet Opens key:

explorer\main\featurecontrol\feature_restricted_zone_when_file_not_found

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_restricted_zone_when_file_not_found

HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd} Opens key:

HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd} Opens key: Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\treatas

 $HKCR\clsid\\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\\{treatas}$ Opens key: Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprocserver32

HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprocserverx86

Opens key:

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\localserver32

 $HKCR\clsid\ensuremath{\clsid}\$ Opens key:

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprochandler32

 $HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\ \ liprochandler 32$ Opens key:

Opens key: HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-

fd2b31b3eefd}\inprochandlerx86

HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\inprochandlerx86 Opens key:

HKCU\software\classes\clsid\{e569bde7-a8dc-47f3-893f-Opens key:

fd2b31b3eefd}\localserver

HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\localserver Opens key:

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature block lmz img Opens key: HKLM\software\microsoft\internet

```
HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options\powrprof.dll
  Opens key:
                                 HKCU\control panel\powercfg
  Opens key:
                                 \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} indows \end{tabular} current version \end{tabular} controls folder \end{tabular} on the label{tabular} and the label{tabular} \begin{tabular}{ll} help the label{tabular} help
  Opens key:
                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:
                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:
                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:
                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:
                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:
                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:
                                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
                                 HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache
  Opens key:
                                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:
                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                                HKCU\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                                HKLM\software\microsoft\internet
  Opens key:
explorer\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
                                HKCU\software\microsoft\internet
  Opens key:
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:
\verb|explorer\main\featurecontrol\feature_disallow_null_in_response\_headers| \\
  Opens key:
                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:
                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:
                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:
                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens key:
                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
  Opens key:
                                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
  Opens key:
                                 HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
Opens kev:
```

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ parameters \ protocol_catalog_entries \ protocol_catalog \ parameters \ parameters$

explorer\main\featurecontrol\feature_block_lmz_img

Opens key:

Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
  Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 0000000000011) \ (catalog\_entries \ (catalog \ (catalog\_entries \ (catalog \ (cata
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
  Opens key:
HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:
                                    HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens kev:
                                    HKCU\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
  Opens key:
                                    HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                                    HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasman.dll
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\winmm.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
  Opens key:
                                    HKLM\software\microsoft\windows\currentversion\telephony
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasapi32.dll
  Opens key:
                                    HKLM\software\microsoft\tracing\rasapi32
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
                                    HKLM\system\currentcontrolset\control\productoptions
  Opens key:
  Opens key:
                                    \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}
folders
  Opens kev:
                                    HKLM\software\policies\microsoft\windows\system
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:
                                    HKLM\system\currentcontrolset\control\session manager\environment
                                    Opens key:
1757981266-507921405-1957994488-1003
  Opens key:
                                    HKCU\environment
                                    HKCU\volatile environment
  Opens kev:
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sensapi.dll
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens key:
options\rasadhlp.dll
  Opens key:
                                    \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution
options\dnsapi.dll
  Opens kev:
                                    HKLM\svstem\currentcontrolset\services\dnscache\parameters
  Opens key:
                                    HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:
                                    HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:
                                    HKLM\software\microsoft\rpc\securityservice
  Opens key:
                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
  Opens key:
                                    HKLM\software\policies\microsoft\cryptography
  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\cryptography
  Opens kev:
                                    HKLM\software\microsoft\cryptography\offload
                                    \label{local_hammon_hammon} \begin{tabular}{ll} HKCU \software \classes \clsid \ \{00021401-0000-0000-c000-000000000046\} \end{tabular}
  Opens key:
                                    HKCR\clsid\{00021401-0000-0000-c000-00000000046}
```

HKCU\software\classes\clsid\{00021401-0000-0000-c000-

Opens key: Opens key:

Opens key:

000000000046}\treatas

Opens key: HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserver32 Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll

Opens key: HKCU\software\classes\clsid\{00021401-0000-0000-c000-

00000000046}\inprocserverx86

Opens key: HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{00021401-0000-0000-c000-

000000000046}\localserver32

Opens key: HKCR\clsid\{00021401-0000-0000-c000-00000000046}\localserver32
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: HKCU\software\classes\clsid\{00021401-0000-0000-c000-

00000000046}\inprochandler32

Opens key: HKCR\clsid\{00021401-0000-0000-c000-00000000046}\inprochandler32

Opens key: HKCU\software\classes\clsid\{00021401-0000-0000-c000-

00000000046}\inprochandlerx86

Opens key: HKCR\clsid\{00021401-0000-0000-0000-00000000046}\inprochandlerx86

Opens key: HKCU\software\classes\clsid\{00021401-0000-0000-c000-

000000000046}\localserver

Opens key: HKCR\clsid\{00021401-0000-0000-0000-00000000046}\localserver

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

options\wshtcpip.dll

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

options\msv1_0.dll

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

Opens key: HKCU\software\classes\.exe

Opens key: HKCR\.exe

Opens key: HKCU\software\classes\exefile

Opens key: HKCR\exefile

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

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

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

Opens key: HKCR\exefile\shellex\iconhandler

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

Opens key: HKCR\systemfileassociations\.exe

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

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

Opens key: HKCR\exefile\clsid

Opens key: HKCU\software\classes*\clsid

Opens key: HKCR*\clsid

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

options\linkinfo.dll

Opens key: HKCU\software\classes\network\sharinghandler

Opens key: HKCR\network\sharinghandler

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

options\ntshrui.dll

 $Opens\ key: \\ HKLM \ system \ current controls et \ services \ land anserver \ defaults ecurity \\$

Opens key: HKCU\software\classes\clsid\{59031a47-3f72-44a7-89c5-

5595fe6b30ee}\inprocserver32

Opens key: HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\inprocserver32

Opens key: HKCU\software\soft-ware

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

options\msimg32.dll

Opens key: HKCU\software\microsoft\internet

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

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

Queries value:

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

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

nt\currentversion\compatibility32[3c8f7cba29f3aa462740dd7998c5cb74]

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

compatibility[3c8f7cba29f3aa462740dd7998c5cb74]

Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]

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

manager[criticalsectiontimeout]

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

Queries value: HKCR\interface[interfacehelperdisableall]

Queries value: HKCR\interface[interfacehelperdisableallforole32]

HKCR\interface[interfacehelperdisabletypelib] Oueries value: HKCR\interface\{00020400-0000-0000-c000-Oueries value: 00000000046}[interfacehelperdisableall] HKCR\interface\{00020400-0000-0000-c000-Queries value: 00000000046}[interfacehelperdisableallforole32] Queries value: HKCU\control panel\desktop[multiuilanguageid] HKCU\control panel\desktop[smoothscroll] Oueries value: Oueries value: HKLM\system\setup[systemsetupinprogress] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips] HKLM\software\microsoft\windows\currentversion\internet Oueries value: settings[disableimprovedzonecheck] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[3c8f7cba29f3aa462740dd7998c5cb74.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*] HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-Queries value: ab78-1084642581fb] Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-0000000000001 Queries value: HKLM\software\microsoft\ctf\systemshared[cuas] Queries value: HKCU\keyboard layout\toggle[language hotkey] HKCU\keyboard layout\toggle[hotkey] Queries value: Queries value: HKCU\keyboard layout\toggle[layout hotkey] Queries value: HKLM\software\microsoft\ctf[enableanchorcontext] HKLM\software\microsoft\windows nt\currentversion\imm[ime file] Oueries value: Queries value: HKCU\software\microsoft\ctf[disable thread input manager] Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Oueries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername] Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Queries value: c7d49d7cecdc}[enabledhcp] Oueries value: $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-4304-4404, and the services \ tcpip \ parameters \ terrange \ terr$ c7d49d7cecdc}[leaseobtainedtime] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[leaseterminatestime] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[dhcpserver] ${\tt HKLM \ } system \verb| current control set \verb| services \verb| ldap[ldapclient integrity]|$ Queries value: Queries value: HKLM\system\wpa\pnp[seed] Queries value: HKLM\system\setup[osloaderpath] Queries value: HKLM\system\setup[systempartition] Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Oueries value: HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath] HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath] Oueries value: HKLM\software\microsoft\windows\currentversion\setup[drivercachepath] HKLM\software\microsoft\windows\currentversion[devicepath] Queries value: Oueries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel] Queries value: HKLM\software\microsoft\windows\currentversion\setup[logpath] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] ${\tt HKLM \backslash system \backslash current control set \backslash services \backslash tcpip \backslash parameters [domain]}$ Oueries value: HKCR\http\shell\open\command[] Oueries value: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[] Queries value: Queries value: HKLM\software\microsoft\com3[com+enabled] Oueries value: ${\tt HKLM \setminus software \setminus microsoft \setminus ole[minimumfree mempercentage to create process]}$ HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject] Queries value: Queries value: HKLM\software\microsoft\com3[regdbversion] HKCR\clsid\{8856f961-340a-11d0-a96b-Oueries value: 00c04fd705a2}\inprocserver32[inprocserver32] Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[] HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[appid] Oueries value: Queries value: HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[threadingmodel] Queries value: HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow] HKLM\software\microsoft\internet Oueries value: explorer\setup[iexplorelastmodifiedhigh]

Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode] Oueries value: HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\tvpelib[] Queries value: HKLM\software\microsoft\internet explorer\setup[installstarted] $HKCR \land eface \land \{b722bccb-4e68-101b-a2bc-00aa00404770\} \land proxystubclsid32[]$ Oueries value: Oueries value: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[] Oueries value: HKCR\interface\{000214e6-0000-0000-c000-00000000046}\proxystubclsid32[] Queries value: $HKCR \ interface \ \{93f2f68c-1d1b-11d3-a30e-00c04f79abd1\} \ proxystubclsid32[]$ Oueries value: HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[] Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]

Oueries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh] HKLM\software\policies\microsoft\internet Oueries value: explorer\security[disablesecuritysettingscheck] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\0[flags] Queries value: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ settings\zones\1[flags] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\zones\2[flags] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3[flags] Queries value: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ settings\zones\4[flags] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[createuricachesize] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings[createuricachesize] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[enablepunycode] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings[enablepunycode] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood] HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders] HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[] Queries value: Oueries value: 11e3-9fc7-806d6172696f}[data] Queries value: 11e3-9fc7-806d6172696f}[generation] Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Queries value: $HKCU \ software \ microsoft \ windows \ current version \ policies \ \ explorer \ [force active desk topon]$ 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] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess] Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] Oueries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu] HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath] Queries value: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} is a constant \cite{tabular} and \cit$ Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] Queries value: $\label{lem:hkcu} \verb+KKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]$ Oueries value: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [shows uper hidden]$ Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Oueries value: $HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [nonetcrawling]$ HKCR\directory[docobject] Oueries value: Queries value: HKCR\directory[browseinplace]

Oueries value: HKCR\directory[isshortcut] HKCR\directory[alwaysshowext] Oueries value: Oueries value: HKCR\directory[nevershowext]

Queries value:

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

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html[progid]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.html[application]

Oueries value: HKCR\.html[]

HKCR\htmlfile\shellex\iconhandler[] Oueries value:

Queries value: HKCR\htmlfile[docobject] Oueries value: HKCR\.html[perceivedtype]

HKCR\systemfileassociations\text[docobject] Oueries value:

Queries value: HKCR\htmlfile[browseinplace]

Queries value: HKCR\systemfileassociations\text[browseinplace]

Oueries value: HKCR\htmlfile\clsid[] Queries value: HKCR\htmlfile[isshortcut]

Oueries value: HKCR\systemfileassociations\text[isshortcut]

Oueries value: HKCR\htmlfile[alwaysshowext]

Queries value: HKCR\systemfileassociations\text[alwaysshowext]

Queries value: HKCR\htmlfile[nevershowext]

Oueries value: HKCR\svstemfileassociations\text[nevershowext]

Queries value: HKCU\software\microsoft\internet explorer\main[frametabwindow] Queries 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] Queries value: HKCU\software\microsoft\internet explorer\main[sessionmerging] ${\tt HKLM \setminus software \setminus microsoft \setminus internet \ explorer \setminus main[sessionmerging]}$ Oueries value: Queries value: HKCU\software\microsoft\internet explorer\main[admintabprocs] HKLM\software\microsoft\internet explorer\main[admintabprocs] Oueries value:

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

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

Oueries value:

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

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

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

settings[urlencoding]

HKCU\software\microsoft\internet explorer\international[acceptlanguage] Queries value:

Oueries value:

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

Oueries value: HKLM\software\microsoft\windows\currentversion\policies\ratings[kev]

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

settings[specialfolderscachesize]

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

settings[specialfolderscachesize]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache]

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

Queries value:

folders[cookies] HKCU\software\microsoft\internet explorer[no3dborder]

Oueries value:

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

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling[3c8f7cba29f3aa462740dd7998c5cb74.exe]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_handling[*]

HKLM\software\microsoft\ole[maximumallowedallocationsize] Oueries value: Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings[proxyenable]

HKCR\.html[content type] Queries value: Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_sniffing[3c8f7cba29f3aa462740dd7998c5cb74.exe]

Oueries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_mime_sniffing[*]

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

settings[istextplainhonored]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_safe_bindtoobject[3c8f7cba29f3aa462740dd7998c5cb74.exe]

HKLM\software\microsoft\internet Oueries value: explorer\main\featurecontrol\feature_safe_bindtoobject[*] HKCR\clsid\{25336920-03f9-11cf-8fd0-Oueries value:

00aa00686f13}\inprocserver32[inprocserver32]

HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\inprocserver32[] Queries value:

Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}[appid]

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

00aa00686f13}\inprocserver32[threadingmodel]

Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_legacy_dispparams[3c8f7cba29f3aa462740dd7998c5cb74.exe]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_legacy_dispparams[*] Oueries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_object_caching[3c8f7cba29f3aa462740dd7998c5cb74.exe]

Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_object_caching[*]

Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]

Queries value: HKLM\software\microsoft\internet explorer\application

compatibility[3c8f7cba29f3aa462740dd7998c5cb74.exe]

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

Queries value: HKCU\software\microsoft\windows

nt\currentversion\windows[dragscrollinset]

Queries value: HKCU\software\microsoft\windows

nt\currentversion\windows[dragscrolldelay]

Queries value: HKCU\software\microsoft\windows

nt\currentversion\windows[dragscrollinterval]

Queries value: HKLM\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature_restrict_filedownload[3c8f7cba29f3aa462740dd7998c5cb74.exe]|$

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_restrict_filedownload[*] Queries value: HKCR\protocols\handler\about[clsid] Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-

00aa00bdce0b}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}\inprocserver32[]

Queries value: HKCR\clsid\{3050f406-98b5-11cf-bb82-00aa00bdce0b}[appid]

Queries 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] Queries value: HKCR\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\progid[]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_legacy_dlcontrol_behaviors[3c8f7cba29f3aa462740dd7998c5cb74.exe]

Queries value: HKLM\software\microsoft\internet

 $\verb|explorer\main\featurecontrol\feature_legacy_dlcontrol_behaviors[*]|$

Queries value: HKLM\software\policies\microsoft\internet explorer[smartdithering]
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]

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

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

explorer\main[page_transitions]

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

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

explorer\main[use_dlgbox_colors]

Queries value: HKCU\software\microsoft\internet explorer\main[use_dlgbox_colors] Queries value: HKLM\software\policies\microsoft\internet explorer\main[anchor

underline]

Queries value: HKCU\software\microsoft\internet explorer\main[anchor underline]
Queries value: HKCU\software\microsoft\internet explorer\main[css_compat]
Queries value: HKCU\software\microsoft\internet explorer\main[expand alt text]

 $\label{thm:policies} Queries \ value: \\ HKLM \ software \ policies \ microsoft \ internet \ explorer \ main[display inline] \\$

videos]

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

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

explorer\main[play_background_sounds]

Queries value: HKCU\software\microsoft\internet explorer\main[play_background_sounds]
Queries value: HKLM\software\policies\microsoft\internet explorer\main[play_animations]

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

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

explorer\main[print_background]

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

Queries value: HKLM\software\policies\microsoft\internet explorer\main[show image

placeholders]

Queries value: HKCU\software\microsoft\internet explorer\main[show image placeholders] 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]

```
HKCU\software\microsoft\internet explorer\main[usehr]
  Oueries value:
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\main[q300829]
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\main[cleanup htcs]
                                     HKLM\software\policies\microsoft\internet explorer\main[xdomainrequest]
  Queries value:
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\main[xdomainrequest]
  Queries value:
                                     HKLM\software\microsoft\internet explorer\main[xdomainrequest]
  Oueries value:
                                     HKLM\software\policies\microsoft\internet explorer\main[domstorage]
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\main[domstorage]
  Oueries value:
                                     HKLM\software\microsoft\internet explorer\main[domstorage]
  Oueries value:
                                     HKCU\software\microsoft\internet
explorer\international[default_codepage]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\international[autodetect]
  Oueries value:
                                     HKCU\software\microsoft\internet
explorer\international\scripts[default iefontsizeprivate]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\settings[anchor color]
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\settings[anchor color visited]
                                     HKCU\software\microsoft\internet explorer\settings[anchor color hover]
  Oueries value:
  Queries value:
                                     HKCU\software\microsoft\internet explorer\settings[always use my colors]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\settings[always use my font
size1
  Queries value:
                                     HKCU\software\microsoft\internet explorer\settings[always use my font
face]
  Oueries value:
                                     HKCU\software\microsoft\internet explorer\settings[disable visited
hyperlinks]
  Queries value:
                                     HKCU\software\microsoft\internet explorer\settings[use anchor hover
color1
  Queries value:
                                     HKCU\software\microsoft\internet explorer\settings[miscflags]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\policies[allow
programmatic cut_copy_paste]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                                     HKLM\system\currentcontrolset\control\nls\codepage[950]
  Queries value:
                                     HKCU\software\microsoft\internet
  Queries value:
explorer\international\scripts\3[iefontsize]
  Oueries value:
                                     HKCU\software\microsoft\internet
explorer\international\scripts\3[iefontsizeprivate]
  Oueries value:
                                     HKCU\software\microsoft\internet
explorer\international\scripts\3[iepropfontname]
                                     HKCU\software\microsoft\internet
explorer\international\scripts\3[iefixedfontname]
                                     HKLM\software\microsoft\internet explorer\version vector[vml]
  Oueries value:
                                     HKLM\software\microsoft\internet explorer\version vector[ie]
  Queries value:
  Oueries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[3c8f7cba29f3aa462740dd7998c5cb74.exe]
                                     HKLM\software\microsoft\internet
  Oueries value:
explorer\main\featurecontrol\feature_zone_elevation[*]
  Queries value:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[2700]
                                     HKLM\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones\0[2700]
                                     HKLM\software\microsoft\internet
  Queries value:
explorer\main\featurecontrol\feature xssfilter[3c8f7cba29f3aa462740dd7998c5cb74.exe]
  Queries value:
                                     HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_xssfilter[*]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\zones[securitysafe]
  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:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1400]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[warnonintranet]
                                     \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
  Queries value:
settings[warnonintranet]
                                     HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\zonemap[autodetect]
  Queries value:
                                     HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[inprocserver32]
                                     HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}\inprocserver32[]
  Queries value:
                                     HKCR\clsid\{50d5107a-d278-4871-8989-f4ceaaf59cfc}[appid]
  Oueries value:
  Oueries value:
                                     HKCR\clsid\{50d5107a-d278-4871-8989-
f4ceaaf59cfc}\inprocserver32[threadingmodel]
  Queries value:
                                     HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64\\ \label{eq:c9633f71be64} \\ \l
  Queries value:
                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
431b3828ba53}\inprocserver32[inprocserver32]
  Oueries value:
                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}\inprocserver32[]
  Oueries value:
                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-431b3828ba53}[appid]
                                     HKCR\clsid\{3ce74de4-53d3-4d74-8b83-
```

431b3828ba53}\inprocserver32[threadingmodel]

Queries value:

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

```
869523e2d6c7}\inprocserver32[inprocserver32]
                                                         HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}\inprocserver32[]
    Oueries value:
    Oueries value:
                                                          HKCR\clsid\{a4b544a1-438d-4b41-9325-869523e2d6c7}[appid]
    Queries value:
                                                          HKCR\clsid\{a4b544a1-438d-4b41-9325-
869523e2d6c7}\inprocserver32[threadingmodel]
    Queries value:
                                                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[description]
                                                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
    Oueries value:
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[description]
    Oueries value:
                                                         HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80\} \\ category \\ item \\ \{c6debc0a-f2b2-4f17-930e-ca9faff4cd04\} \\ [description]
    Queries value:
                                                         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[recent]
    Queries value:
                                                         HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[inprocserver32]
    Queries value:
                                                          HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}\inprocserver32[]
                                                          HKCR\clsid\{f414c260-6ac0-11cf-b6d1-00aa00bbbb58}[appid]
    Oueries value:
    Queries value:
                                                          HKCR\clsid\{f414c260-6ac0-11cf-b6d1-
00aa00bbbb58}\inprocserver32[threadingmodel]
                                                         HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings\zones\0[1201]
                                                          HKLM\system\currentcontrolset\control\nls\locale[00000409]
    Queries value:
                                                          HKLM \ system \ current controls et \ \ control \ \ language \ groups [1]
    Oueries value:
    Queries value:
                                                          HKLM\software\microsoft\ole[defaultaccesspermission]
    Queries value:
                                                          HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
    Queries value:
                                                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[2000]
                                                          HKCU\software\microsoft\windows\currentversion\internet settings\url
    Queries value:
history[daystokeep]
                                                          \label{localization} \mbox{HKCU\software\mbox{\sc microsoft\ftp[use\ web\ based\ ftp]}}
    Queries value:
                                                          HKCU\software\microsoft\internet
    Oueries value:
explorer\services[selectionactivitybuttondisable]
                                                          HKLM\system\currentcontrolset\control\session
    Queries value:
manager\appcompatibility[disableappcompat]
    Oueries value:
                                                          HKLM\system\wpa\mediacenter[installed]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
    Queries value:
                                                         HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
    Queries value:
be2efd2c1a33}[itemdata]
be2efd2c1a33}[saferflags]
    Oueries value:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{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-9b89-4666f-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-9b89-4666f-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}[itemdata]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
    Oueries value:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{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-9b89-4666f-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-9b89-4666f-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}[itemsize]
    Queries value:
edd5fbde1328}[saferflags]
    Oueries value:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57
b813f72dbb91}[itemdata]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[hashalg]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemsize]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemdata]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[hashalg]
    Queries value:
7c29ddecae3f}[itemsize]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[saferflags]
    Queries value:
085bcc18a68d}[itemdata]
```

Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[hashalg] 085bcc18a68d}[itemsize] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[saferflags] Oueries value: b91490411bfc}[itemdata] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2eb91490411bfc}[hashalg] Oueries value: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe$ b91490411bfc}[itemsize] Queries value: $HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-4$ b91490411bfc}[saferflags] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[cointernetcombineiuricachesize] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_subdownload_lockdown[3c8f7cba29f3aa462740dd7998c5cb74.exe] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_subdownload_lockdown[*] HKCR\.css[content type] Queries value: Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel] HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope] HKCU\software\microsoft\windows\currentversion\explorer\shell Oueries value: folders[cache] Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename] HKLM\software\microsoft\internet explorer\default behaviors[discovery] HKCR\clsid\{3050f4cf-98b5-11cf-bb82-Queries value: 00aa00bdce0b}\inprocserver32[inprocserver32] $\label{local-bb82-00aa00bdce0b} Linprocserver 32[] \\$ Queries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-00aa00bdce0b}[appid] Oueries value: HKCR\clsid\{3050f4cf-98b5-11cf-bb82-Oueries value: 00aa00bdce0b}\inprocserver32[threadingmodel] HKCR\.png[content type] Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-Oueries value: 00aa006c1a01}\inprocserver32[inprocserver32] HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}\inprocserver32[] Oueries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-00aa006c1a01}[appid] Queries value: HKCR\clsid\{30c3b080-30fb-11d0-b724-Oueries value: 00aa006c1a01}\inprocserver32[threadingmodel] HKCR\clsid\{6a01fda0-30df-11d0-b724-Queries value: 00aa006c1a01}\inprocserver32[inprocserver32] Oueries value: HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}\inprocserver32[] HKCR\clsid\{6a01fda0-30df-11d0-b724-00aa006c1a01}[appid] Queries value: HKCR\clsid\{6a01fda0-30df-11d0-b724-Oueries value: 00aa006c1a01}\inprocserver32[threadingmodel] HKCR\mime\database\content type\image/bmp\bits[0] Oueries value: Queries value: HKCR\mime\database\content type\image/gif\bits[0] Queries value: HKCR\mime\database\content type\image/jpeg\bits[0] Oueries value: HKCR\mime\database\content type\image/pjpeg\bits[0] HKCR\mime\database\content type\image/png\bits[0] Queries value: Queries value: HKCR\mime\database\content type\image/x-png\bits[0] HKCR\mime\database\content type\image/x-wmf\bits[0] Queries value: HKCR\mime\database\content type\image/x-png[image filter clsid] Oueries value: Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[inprocserver32] Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[] HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}[appid] Oueries value: Queries value: HKCR\clsid\{a3ccedf7-2de2-11d0-86f4-00a0c913f750}\inprocserver32[threadingmodel] HKCR\.gif[content type] Oueries value: Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[syncmode5] HKLM\software\microsoft\windows\currentversion\internet Oueries value: settings\5.0\cache[sessionstarttimedefaultdeltasecs] HKCU\software\microsoft\windows\currentversion\internet Oueries value:

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[signature]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]

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

settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]

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

Queries value:

```
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                          \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
 Queries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Queries value:
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-
fd2b31b3eefd}\inprocserver32[inprocserver32]
                           HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd}\ \ inprocserver 32[]
 Queries value:
 Oueries value:
                           HKCR\clsid\{e569bde7-a8dc-47f3-893f-fd2b31b3eefd\}[appid]
                          HKCR\clsid\{e569bde7-a8dc-47f3-893f-
 Oueries value:
fd2b31b3eefd}\inprocserver32[threadingmodel]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
 Queries value:
                           HKCU\control panel\powercfg[adminmaxsleep]
                           HKCU\control panel\powercfg[adminmaxvideotimeout]
 Queries value:
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\controls
folder\powercfg[lastid]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[fromcachetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[secureprotocols]
                           HKLM\software\policies\microsoft\internet
 Queries value:
explorer\main[security_hklm_only]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablekeepalive]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disablepassport]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[idnenabled]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[cachemode]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[proxyhttp1.1]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablenegotiate]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
                          HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Queries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature clientauthcertfilter]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disableworkerthreadhibernation]
 Queries value:
                          \label{lem:hklm} \verb+ HKLM \software \microsoft \windows \current version \cite{thmosoft} internet
settings[disableworkerthreadhibernation]
 Queries 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]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxhttpredirects]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[maxconnectionsperserver]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1 Oserver]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[serverinfotimeout]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[connectretries]
```

```
Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                            HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[receivetimeout]
 Queries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                            HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablentlmpreauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certcachenovalidate]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelifetime]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[ftpdefaultexpirytimesecs]
                            HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[3c8f7cba29f3aa462740dd7998c5cb74.exe]
 Oueries value:
                           HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[perusercookies]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[leashlegacycookies]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
                            HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dialupuselansettings]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypassftptimecheck]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[releasesocketduring401auth]
 Oueries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablelegacypreauthasserver]
 Queries value:
                            HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
 Oueries value:
                            HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                            \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
 Queries value:
settings[bvpasssslnocachecheck]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
                            HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
 Queries value:
                            \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[nocheckautodialoverride]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[dontusednsloadbalancing]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dontusednsloadbalancing]
 Queries value:
                            \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + internet
settings[sharecredswithwinhttp]
 Queries value:
                            \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[mimeexclusionlistforcache]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[headerexclusionlistforcache]
 Queries value:
                           \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
settings[dnscacheenabled]
```

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

Queries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ (catalog_entries \ 000000000003 \ [displaystring]$ Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily] Oueries value:

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

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[globaluseroffline]

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

settings[enableautodial]

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

settings[urlencoding]

Queries value: Queries value:

Oueries value:

Queries value:

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

settings[truncatefilename]

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

settings[badproxyexpirestime]

HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midil Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Queries value: Oueries value: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi4]$ $HKLM \backslash software \backslash microsoft \backslash windows \ nt \backslash current version \backslash drivers 32 [midi5]$ Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi91 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]

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

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

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2] Oueries value: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ drivers 32 [mixer 3]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9] Queries value:

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

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

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

Oueries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell

folders[common appdata]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\winlogon[userenvdebuglevel]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[chkaccdebuglevel]

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

folders[personal]

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

folders[local settings]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[rsopdebuglevel]

HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] Queries value:

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\profilelist[profilesdirectory]

HKLM\software\microsoft\windows Queries value:

nt\currentversion\profilelist[allusersprofile]

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

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

Queries value:

1757981266-507921405-1957994488-1003[profileimagepath] HKCU\software\microsoft\windows

nt\currentversion\winlogon[parseautoexec]

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

folders[appdata]

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

settings[migrateproxy]

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

settings\connections[savedlegacysettings]

Queries value: $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc urrentversion\sc internet}} \\$

settings\connections[defaultconnectionsettings]

HKLM\svstem\currentcontrolset\services\winsock2\parameters[autodialdll] Oueries value:

Oueries value:

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

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]

Queries value: $HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters| [prioritize record data]|$

Queries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]

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

Oueries value:

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

Oueries value:

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

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

Queries value:

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

Oueries value:

Queries value:

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

HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries value:

Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]

Oueries value:

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

Queries value:

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

Oueries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones] HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicast listen level]$ HKLM\svstem\currentcontrolset\services\dnscache\parameters[multicastsendlevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquick query time outs]$ HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[queryadaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[disableadapterdomainname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registrationenabled] Oueries value: c7d49d7cecdc}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[registrationmaxaddresscount] Oueries value: c7d49d7cecdc}[maxnumberofaddressestoregister] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[domain] Queries value: c7d49d7cecdc}[dhcpdomain] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[ipautoconfigurationenabled] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3c7d49d7cecdc}[addresstype] Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-

c7d49d7cecdc}[nameserver]

Queries value:

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
                          HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
 Queries value:
                          HKLM \ software \ microsoft \ cryptography \ defaults \ provider \ microsoft \ strong
cryptographic provider[type]
                          HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
 Oueries value:
cryptographic provider[image path]
                          HKLM\software\microsoft\rpc\securityservice[10]
 Queries value:
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
 Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
 Oueries value:
HKLM\system\currentcontrol\set\control\lsa\sspicache\msapsspc.dl1[comment]
 Queries value:
                          HKLM\software\microsoft\cryptography[machineguid]
 Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
 Queries value:
HKLM\system\currentcontrol\set\control\lsa\sspicache\msapsspc.dll[version]
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
 Queries value:
 Queries value:
HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus msapsspc.dll[tokensize]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
                          HKCR\clsid\{00021401-0000-0000-c000-
 Queries value:
00000000046}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{00021401-0000-0000-c000-0000000046}\inprocserver32[]
 Queries value:
                          HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
                          HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
 Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
                          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
 Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [used elayed acceptance]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                          HKCR\clsid\{00021401-0000-0000-c000-00000000046}[appid]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
 Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
 Oueries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
                          HKLM \setminus system \setminus current control \\ \  \mid sa \setminus sspicache \setminus msnsspc.dll[version]
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
                          HKCR\clsid\{00021401-0000-0000-c000-
 Queries value:
00000000046}\inprocserver32[threadingmodel]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
 Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\user shell
 Oueries value:
folders[common documents]
                          HKLM\software\microsoft\windows\currentversion\explorer\user shell
 Queries value:
folders[common desktop]
                          HKCR\.exe[]
 Oueries value:
                          HKCR\exefile[docobject]
 Queries value:
 Queries value:
                          HKCR\exefile[browseinplace]
 Queries value:
                          HKCR\exefile[isshortcut]
 Oueries value:
                          HKCR\exefile[alwaysshowext]
 Queries value:
                          HKCR\exefile[nevershowext]
 Queries value:
                          HKCR\network\sharinghandler[]
 Queries value:
HKLM\system\currentcontrolset\services\lanmanserver\defaultsecurity[srvsvcdefaultshareinfo]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[start menu]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common start menu]
```

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

Queries value:

folders[my pictures]

HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)] Oueries value: $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} windows \end{tabular} current version \end{tabular} explorer \end{tabular} user shell$ Oueries value:

folders[commonpictures]

HKCR\clsid\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\inprocserver32[] Oueries value:

Queries value:

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

HKLM\software\microsoft\windows\currentversion\explorer\user shell Oueries value:

folders[commonmusic]

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

folders[commonvideo]

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

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

settings\zones\3[1a00]

Value changes: HKLM\software\microsoft\cryptography\rng[seed]

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

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]

Value changes:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints \\ 2 \setminus \{f90255c2-6bc4-11e3-9fc7-12e3-12e4\} \setminus factor \\ 2 \setminus \{f90255c2-6bc4-11e3-9fc7-12e4\} \setminus factor \\ 3 \setminus \{f90255c2-6bc4-11e3-9fc7-12e4\} \setminus factor \\ 4 \setminus \{f9025c2-6bc4-11e3-9fc7-12e4\} \setminus factor \\ 4 \setminus \{f9025c2-6bc4-12e4\} \setminus factor \\ 4 \setminus \{f9025c2-6bc4-12e4\} \setminus factor \\ 4 \setminus \{f9025c2-6bc4-12e4\} \setminus factor \\ 4 \setminus \{f9025c2$

806d6172696f}[baseclass]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

HKCU\software\microsoft\windows\currentversion\explorer\shell Value changes:

folders[cookies]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[history]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[local appdata]

Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell

folders[common appdata]

Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[appdata]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

HKCU\software\microsoft\windows\currentversion\explorer\shell Value changes:

folders[desktop]

HKCU\software\microsoft\windows\currentversion\explorer\shell Value changes: folders[personal]

Value changes: $\label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ windows\+ current version\+ explorer\+ shell$

folders[common documents] Value changes:

HKLM\software\microsoft\windows\currentversion\explorer\shell

folders[common desktop]

HKCU\software\microsoft\windows\currentversion\explorer\shell Value changes: folders[start menul

Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell

folders[common start menu]

Value changes:

HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my

pictures]

Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell

folders[commonpictures]

HKLM\software\microsoft\windows\currentversion\explorer\shell Value changes:

folders[commonmusic]

Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell

folders[commonvideo]