# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 1, Task ID: 4

Task ID: 4
Risk Level: 10

Date Processed: 2016-03-28 07:35:10 (UTC)

Processing Time: 65.77 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\spyeye\_injector.exe"

Sample ID: 1
Type: basic
Owner: admin

Label: spyeye\_injector.exe
Date Added: 2016-03-28 07:35:09 (UTC)

File Type: PE32:win32:gui File Size: PE32:win32:gui

MD5: b98bb6d7428c3dbffcfcab2414c6daa2

SHA256: fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029

Description: None

## Pattern Matching Results

7 Writes to memory of system processes

- 6 Modifies registry autorun entries 3 HTTP connection - response code 200 (success)
- 2 PE: Nonstandard section
- 5 Abnormal sleep detected
- 6 Renames file on boot
- 3 Connects to local host
- 10 Suspicious writeprocess: Spyeye [Banking]
- 4 Terminates process under Windows subfolder
- 4 Reads process memory
- 5 PE: Contains compressed section
- 6 Notifies system about Internet connection change
- 3 Program causes a crash [Info]
- 5 Packer: UPX
- 5 Adds autostart object
- 10 Creates malicious mutex: Spyeye [Banking]

#### Static Events

Anomaly: PE: Contains a virtual section
Anomaly: PE: Contains one or more non-standard sections
Packer: UPX

#### Process/Thread Events

Creates process: C:\windows\temp\spyeye\_injector.exe

["C:\windows\temp\spyeye\_injector.exe" ]

Creates process: C:\WinOldFileq\83A49421CBD.exe ["C:\WinOldFileq\83A49421CBD.exe"]

Creates process: C:\Users\Admin\AppData\Local\Temp\UK1822B.exe

["C:\Users\Admin\AppData\Local\Temp\UK1822B.exe"]

Creates process: C:\Windows\SysWOW64\rundl132.exe ["C:\Windows\system32\rundl132.exe"

"C:\Windows\syswow64\WININET.dll",DispatchAPICall 1 ]
Reads from process: PID:340 C:\Windows\explorer.exe
Reads from process: PID:348 C:\Windows\System32\wininit.exe
Reads from process: PID:400 C:\Windows\System32\winlogon.exe

Reads from process: PID:452 C:\Windows\System32\lsass.exe PID:460 C:\Windows\System32\lsm.exe Reads from process: PID:564 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:632 C:\Windows\System32\svchost.exe Reads from process: PID:684 C:\Windows\System32\svchost.exe PID:804 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:848 C:\Windows\System32\svchost.exe Reads from process: PID:952 C:\Windows\System32\svchost.exe Reads from process: PID:884 C:\Windows\System32\dwm.exe Reads from process: PID:1088 C:\Windows\System32\spoolsv.exe Reads from process: PID:1188 C:\Windows\System32\taskhost.exe PID:1236 C:\Windows\System32\svchost.exe Reads from process: Reads from process: PID:1332 C:\Windows\System32\svchost.exe Reads from process: PID:1392 C:\Windows\System32\svchost.exe Reads from process: PID:1752 C:\Windows\System32\UIODetect.exe

Reads from process: PID:1888 C:\Windows\System32\mobsync.exe
Reads from process: PID:1712 C:\Windows\System32\mobsync.exe
Reads from process: PID:1556 C:\Windows\System32\rundl132.exe
Reads from process: PID:828 C:\Windows\System32\taskhost.exe

Reads from process: PID:356 C:\Windows\System32\wsqmcons.exe
Reads from process: PID:820 C:\Windows\System32\sdclt.exe
Reads from process: PID:748 C:\Windows\System32\taskhost.exe
Reads from process: PID:516 C:\Windows\System32\wbem\unsecapp.exe

Reads from process: PID:948 C:\Windows\System32\WinSAT.exe

Reads from process:	PID:1604 C:\Windows\System32\conhost.exe
Reads from process:	PID:1716 C:\Windows\System32\wbem\WmiPrvSE.exe
Reads from process:	PID:2072 C:\Windows\System32\conhost.exe
Writes to process:	PID:1224 C:\Program Files (x86)\Adobe\Reader 9.0\Reader\reader_sl.exe
Writes to process:	PID:2132 C:\Users\Admin\AppData\Local\Temp\UK1822B.exe
Writes to process:	PID:2412 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2528 C:\Windows\SysWOW64\WerFault.exe
Writes to process:	PID:2576 C:\Windows\SysWOW64\rundll32.exe
Writes to process:	PID:2608 C:\Windows\SysWOW64\rundll32.exe
Terminates process:	C:\Windows\Temp\spyeye_injector.exe
Terminates process:	C:\WinOldFileq\83A49421CBD.exe
Terminates process:	C:\Windows\SysWOW64\WerFault.exe
Terminates process:	C:\Windows\SysWOW64\rundll32.exe

### Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex	
Creates mutex:	\BaseNamedObjects\RPCController	
Creates mutex:	\Sessions\1\BaseNamedObjects\zXeRY3a_PtW 00000000	
Creates mutex:	\Sessions\1\BaseNamedObjects\_!MSFTHISTORY!_	
Creates mutex:		

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet

Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies! Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!

\BaseNamedObjects\KEEG5mWCUOEqECSCCKYUW5eGQYQWM75 Creates mutex: \Sessions\1\BaseNamedObjects\WininetStartupMutex Creates mutex: \Sessions\1\BaseNamedObjects\WininetConnectionMutex Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex

\Sessions\1\BaseNamedObjects\RasPbFile Creates mutex:

\Sessions\1\BaseNamedObjects\ZonesCounterMutex Creates mutex:

Creates mutex: \Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex \Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex Creates mutex:

 $\verb|\Sessions|| 1 \\ | BaseNamedObjects|| ZonesLockedCacheCounterMutex||$ Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\!IETld!Mutex

\Sessions\1\BaseNamedObjects\\_!MSFTHISTORY!\_LOW!\_ Creates mutex: Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet

files!low!content.ie5! Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!low! Creates mutex:

\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!low!history.ie5!

Creates event: \BaseNamedObjects\SvcctrlStartEvent\_A3752DX Creates event: \Security\LSA\_AUTHENTICATION\_INITIALIZED \KernelObjects\SystemErrorPortReady Creates event:

Creates event: \BaseNamedObjects\BFE\_Notify\_Event\_{60da9867-8164-4cc4-875b-

7060bfd9bbe7}

\Sessions\1\BaseNamedObjects\4FBEA4B1 Creates semaphore:

## File System Events

Creates:	C:\WinOldFileq
Creates:	C:\WinOldFileq\
Creates:	C:\WinOldFileq\83A49421CBD.exe
Creates:	C:\WinOldFileq\8FDC7C717274206
Creates:	<pre>C:\Users\Admin\AppData\Local\Temp\</pre>
Creates:	<pre>C:\Users\Admin\AppData\Local\Temp\UK1822B.tmp</pre>
Creates:	<pre>C:\Users\Admin\AppData\Local\Temp\UK1822B.exe</pre>
Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Local
Creates:	<pre>C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files</pre>
Creates:	<pre>C:\Users\Admin\AppData\Roaming</pre>
Creates:	<pre>C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies</pre>

C:\Users\Admin\AppData\Local\Microsoft\Windows\History Creates: Creates: C:\Users\Admin\Favorites

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE Creates: Creates:  $C: \verb|\USers\Admin\AppData\Roaming\Microsoft\Windows\IETld\Cache|\\$ Creates: C:\Windows\Prefetch\SPYEYE\_INJECTOR.EXE-619282B0.pf Opens:

C:\Windows Opens:

Opens: C:\Windows\System32\wow64.dll Opens: C:\Windows\System32\wow64win.dll C:\Windows\System32\wow64cpu.dll Opens: Opens: C:\Windows\system32\wow64log.dll

Opens: C:\Windows\SysWOW64

Opens: C:\Windows\SysWOW64\sechost.dll Opens: C:\Windows\SysWOW64\kernel32.dll

Opens:

C:\Windows\Globalization\Sorting\SortDefault.nls Opens:

Opens: C:\Windows\SysWOW64\ntdll.dll

Opens: C:\WinOldFileq

```
C:\WinOldFileq\
 Opens:
                         C:\Windows\Temp\spyeye_injector.exe
 Opens:
 Opens:
                         C:\WinOldFileq\83A49421CBD.exe
 Opens:
                         C:\Windows\SysWOW64\apphelp.dll
 Opens:
                         C:\Windows\AppPatch\sysmain.sdb
                         C:\WinOldFileq\ui\SwDRM.dll
 Opens:
                         C:\Windows\Prefetch\83A49421CBD.EXE-8B5C1E36.pf
 Opens:
                         C:\Windows\SysWOW64\imm32.dll
 Opens:
                         C:\WinOldFileq\MSIMG32.dll
 Opens:
                         C:\Windows\SysWOW64\msimg32.dll
 Opens:
 Opens:
                         C:\WinOldFileq\8FDC7C717274206
 Opens:
                         C:\Users\Admin\AppData\Local\Temp
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\UK1822B.exe
 Opens:
                         C:\Users
 Opens:
                         C:\Users\Admin
                         C:\Users\Admin\AppData
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\ui\SwDRM.dll
 Opens:
                         C:\Windows\Prefetch\UK1822B.EXE-A2CDAF51.pf
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\MSIMG32.dll
 Opens:
                         C:\windows\temp\spyeye_injector.exe
 Opens:
                         C:\Program Files (x86)\Adobe\Reader 9.0\Reader\MSIMG32.dll
 Opens:
                         C:\Windows\SysWOW64\user32.dll
 Opens:
                         C:\Windows\SysWOW64\wininet.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\USERENV.dll
                         C:\Windows\SysWOW64\userenv.dll
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\profapi.dll
 Opens:
                         C:\Windows\SysWOW64\profapi.dll
 Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\UK1822B.exe.Local\
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
 Opens:
                         C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
                         C:\Windows\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs
                         Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
 Opens:
Files\Content.IE5\desktop.ini
                         C:\Users\Admin\AppData\Roaming
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
 Opens:
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
 Opens:
                        C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
 Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
                         C:\Windows\SysWOW64\ws2 32.dll
 Opens:
                         C:\Windows\SysWOW64\advapi32.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\crypt32.dll
 Opens:
                         C:\Windows\SysWOW64\tzres.dll
 Opens:
                         C:\Windows\SysWOW64\en-US\tzres.dll.mui
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\dnsapi.DLL
 Opens:
                         C:\Windows\SysWOW64\dnsapi.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\iphlpapi.DLL
 Opens:
                         C:\Windows\SysWOW64\IPHLPAPI.DLL
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\WINNSI.DLL
                         C:\Windows\SysWOW64\winnsi.dll
 Opens:
 Opens:
                         C:\Windows\SysWOW64\mswsock.dll
 Opens:
                         C:\Windows\SysWOW64\WSHTCPIP.DLL
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\RASAPI32.dll
 Opens:
                         C:\Windows\SysWOW64\rasapi32.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\rasman.dll
 Opens:
                         C:\Windows\SysWOW64\rasman.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\rtutils.dll
                         C:\Windows\SysWOW64\rtutils.dll
 Opens:
 Opens:
                         C:\ProgramData\Microsoft\Network\Connections\Pbk\
 Opens:
                         C:\Windows\SysWOW64\ras
 Opens:
                         C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
 Opens:
                         C:\Users\Admin\AppData\Local\Temp\sensapi.dll
 Opens:
                         C:\Windows\SysWOW64\SensApi.dll
 Opens:
                         C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
```

Files\Low

```
C:\Users\Admin\AppData\Local\Microsoft\Windows
  Opens:
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low
  Opens:
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows
  Opens:
  Opens:
                                      C:\Users\Admin\AppData\Roaming\Microsoft
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low
  Opens:
                                      C:\Users\Admin\Favorites
                                      {\tt C:\Windows\Temporary\ Internet}
  Opens:
Files\Virtualized
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE
  Opens:
  Opens:
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows\PrivacIE\Low
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache
  Opens:
  Opens:
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IECompatCache\Low
                                      {\tt C: \tt Vsers \tt Admin \tt AppData \tt Roaming \tt Microsoft \tt Windows \tt IETIdCache}
  Opens:
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows\IETldCache\Low
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\Low
  Opens:
  Opens:
                                      C:\Windows\SysWOW64\rundll32.exe
  Opens:
                                      C:\Windows\SysWOW64\ui\SwDRM.dll
  Opens:
                                      C:\Windows\Prefetch\RUNDLL32.EXE-87432CEE.pf
                                      C:\Windows\SysWOW64\nlaapi.dll
  Opens:
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\rasadhlp.dll
  Opens:
                                      C:\Windows\SysWOW64\rasadhlp.dll
  Opens:
                                      C:\Windows\SysWOW64\WerFault.exe.Local\
  Opens:
                                      C:\Windows\SysWOW64\Faultrep.dll
  Opens:
                                      C:\Windows\SysWOW64\en-US\WerFault.exe.mui
                                      C:\Windows\SysWOW64\uxtheme.dll
  Opens:
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\wkscli.dll
  Opens:
                                      C:\Windows\SysWOW64\wkscli.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\netutils.dll
  Opens:
                                      C:\Windows\SysWOW64\netutils.dll
  Opens:
                                      C:\Windows\SysWOW64\wship6.dll
                                      {\tt C:\Users\Admin\AppData\Local\Temp\dhcpcsvc6.DLL}\\
  Opens:
  Opens:
                                      C:\Windows\SysWOW64\dhcpcsvc6.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\dhcpcsvc.DLL
  Opens:
                                      C:\Windows\SysWOW64\dhcpcsvc.dll
  Opens:
                                      C:\Windows\System32\drivers\etc\hosts
  Opens:
                                      C:\Windows\SysWOW64\FWPUCLNT.DLL
  Opens:
                                      C:\Windows\SysWOW64\NapiNSP.dll
  Opens:
                                      C:\Windows\SysWOW64\pnrpnsp.dll
  Opens:
                                      C:\Windows\SysWOW64\winrnr.dll
                                      C:\Users\Admin\AppData\Local\Temp\ntmarta.dll
  Opens:
  Opens:
                                      C:\Windows\SysWOW64\ntmarta.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\VERSION.dll
                                      C:\Windows\SysWOW64\version.dll
  Opens:
  Opens:
                                      C:\Windows\SysWOW64\en-US\urlmon.dll.mui
  Opens:
                                      C:\Windows\AppPatch\AcLayers.dll
                                      C:\Windows\SysWOW64\winspool.drv
  Opens:
  Opens:
                                      C:\Windows\SysWOW64\mpr.dll
                                      C:\Windows\AppPatch\acwow64.dll
  Opens:
                                      C:\Windows\SysWOW64\en-US\rundll32.exe.mui
  Opens:
  Opens:
                                      C:\Windows\syswow64\WININET.dll.manifest
  Opens:
                                      C:\Windows\SysWOW64\dwmapi.dll
  Opens:
                                      C:\Windows\SysWOW64\rundll32.exe.Local\
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\desktop.ini
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Low\Content.IE5\desktop.ini
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\desktop.ini
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\Low\History.IE5\desktop.ini
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Low\Content.IE5\index.dat
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
  Opens:
\verb|C:|Users\land Admin\land AppData\land Local\land Microsoft\land Windows\land History\land Low\land History. IE5\land index. data for the property of the prope
  Writes to:
                                      C:\WinOldFileq\83A49421CBD.exe
                                      C:\WinOldFileq\8FDC7C717274206
  Writes to:
  Writes to:
                                      C:\Users\Admin\AppData\Local\Temp\UK1822B.exe
  Reads from:
                                      C:\Windows\SysWOW64\ntdll.dll
  Reads from:
                                      C:\Windows\Temp\spyeye injector.exe
                                      C:\WinOldFileq\83A49421CBD.exe
  Reads from:
  Reads from:
                                      C:\WinOldFileq\8FDC7C717274206
  Reads from:
                                      C:\Users\Admin\AppData\Local\Temp\UK1822B.exe
  Reads from:
                                      C:\Windows\SysWOW64\user32.dll
                                      C:\Windows\SysWOW64\wininet.dll
  Reads from:
                                      C:\Windows\SysWOW64\ws2_32.dll
  Reads from:
  Reads from:
                                      C:\Windows\SysWOW64\advapi32.dll
  Reads from:
                                      C:\Windows\SysWOW64\crypt32.dll
```

C:\Windows\SysWOW64\rundll32.exe

C:\Windows\System32\drivers\etc\hosts

Reads from: Reads from: Deletes:

#### Network Events

DNS query: alexeyartemov.com DNS query: www.microsoft.com DNS response: alexeyartemov.com  $\Rightarrow$  198.105.244.11 DNS response: alexeyartemov.com  $\Rightarrow$  104.239.213.7 DNS response: e10088.dspb.akamaiedge.net  $\Rightarrow$  23.221.32.209 e10088.dspb.akamaiedge.net ⇒ 184.86.231.62 DNS response: DNS response: e10088.dspb.akamaiedge.net ⇒ 23.7.35.22 DNS response: e10088.dspb.akamaiedge.net  $\Rightarrow$  104.66.4.137 Connects to: 88.198.13.147:443 Connects to: 104.239.213.7:80 Connects to: 0.0.0.0:80 127.0.0.1:80 Connects to: Connects to: 23.7.35.22:80 Connects to: 104.66.4.137:80 Sends data to: 8.8.8.8:53 Sends data to: 88.198.13.147:443 Sends data to: 4.2.2.1:53 alexeyartemov.com:80 (104.239.213.7) Sends data to: Sends data to: e10088.dspb.akamaiedge.net:80 (23.7.35.22) e10088.dspb.akamaiedge.net:80 (104.66.4.137) Sends data to: Receives data from: 8.8.8.8:53 Receives data from: 4.2.2.1:53 alexeyartemov.com:80 (104.239.213.7) Receives data from: Receives data from: e10088.dspb.akamaiedge.net:80 (23.7.35.22) e10088.dspb.akamaiedge.net:80 (104.66.4.137) Receives data from:

Windows Registry Events				
Creates key:	HKLM\system\currentcontrolset\control\session manager			
Creates key:	HKCU\software\microsoft\windows\currentversion\run			
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings</pre>			
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\0</pre>			
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\1</pre>			
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\2</pre>			
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\3</pre>			
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet settings\zones\4</pre>			
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>			
settings\lockdown_zones	\1			
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>			
settings\lockdown_zones	settings\lockdown_zones\2			
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>			
settings\lockdown_zones\3				
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>			
settings\lockdown_zones	\4			
Creates key:	<pre>HKCU\software\microsoft\internet explorer\phishingfilter</pre>			
Creates key:	HKCU\software\microsoft\internet explorer\recovery			
Creates key:	<pre>HKCU\software\microsoft\systemcertificates\my</pre>			
Creates key:	HKCU\software\microsoft windows			
Creates key:	<pre>HKLM\software\wow6432node\microsoft\tracing</pre>			
Creates key:	<pre>HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32</pre>			
Creates key:	<pre>HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasmancs</pre>			
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>			
settings\connections				
Creates key:	HKCU\software\appdatalow			
Creates key:	HKCU\software\microsoft\internet explorer\internetregistry			
Creates key:	<pre>HKCU\software\microsoft\internet explorer\lowregistry</pre>			
Creates key:	HKCU\software\microsoft\internet			
explorer\lowregistry\dontshowmethisdialogagain				
Creates key:	<pre>HKCU\software\microsoft\windows\currentversion\internet</pre>			
settings\5.0\lowcache				
Creates key:	HKCU\software\microsoft\internet explorer\intelliforms			
Creates key:	HKCU\software\microsoft\internet explorer\toolbar			
Creates key:	HKCU\software\microsoft\internet explorer\toolbar\webbrowser			
Creates key:				
	\windows\currentversion\explorer\menuorder\favorites			
Creates key:	HKCU\software\microsoft\internet explorer\pagesetup			
Creates key:	HKCU\software\microsoft\windows\currentversion\internet			

Creates key: HKCU\software\microsoft\windows\currentversion\explorer\lowregistry Creates key:

settings\passport\lowdamap HKCU\software\microsoft\windows\currentversion\internet settings\wpad

HKCU\software\microsoft\internet explorer\zoom

Creates key:  $\label{lem:hkcu} \mbox{\sc HKCU\software\mbox{\sc microsoft\internet explorer\browseremulation\lowmic}} \mbox{\sc microsoft\sc explorer\sc microsoft\sc explorer\sc explorer$ 

Creates key: HKCU\software\microsoft\internet explorer\ietld\lowmic

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

awareness

Creates key:

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

settings\p3p\history

Creates key: HKLM\software\wow6432node

HKLM\software\wow6432node\microsoft Creates key:

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

settings[proxyserver]

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

settings[proxyoverride]

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

settings[autoconfigurl]

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

settings\zonemap[proxybypass]

Deletes value: 

settings\zonemap[proxybypass]

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

settings\zonemap[intranetname]

Deletes value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\zonemap[intranetname]

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

options

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

Opens key: HKLM\software\microsoft\wow64

Opens key: 

execution options

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

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

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

Opens key: HKLM\system\currentcontrolset\control\nls\customlocale HKLM\system\currentcontrolset\control\nls\language Opens key: Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: HKLM\software\policies\microsoft\mui\settings

Opens key:

Opens key:  $\label{lem:hkcu} \begin{tabular}{ll} HKCU\control\ panel\desktop\muicached\machinelanguageconfiguration \end{tabular}$ Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

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

Opens key: HKCU\control panel\desktop

HKCU\control panel\desktop\muicached Opens key:

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

HKI M\ Opens key:

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\diagnostics

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

Opens key: 

Opens key: HKLM\svstem\setup

Opens key:

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

options\83a49421cbd.exe

HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers  $\label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\windows} nt\current\version\app\compatflags\layers} \\$ Opens key:

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\83a49421cbd.exe

Opens key: HKLM\system\currentcontrolset\services\crypt32 Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\gre\_initialize

 $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows$ Opens key:

nt\currentversion\compatibility32

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime

compatibility

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows

Opens key: HKLM\software\wow6432node\microsoft\ole Opens key: HKLM\software\wow6432node\microsoft\ole\tracing

Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\wow6432node\microsoft\oleaut

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key:

settings Opens kev:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings HKLM\software\policies\microsoft\windows\currentversion\internet Opens key:

settings

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

options\uk1822b.exe

HKLM\software\microsoft\windows Opens key: nt\currentversion\appcompatflags\custom\uk1822b.exe

Opens key: HKLM\software\wow6432node\microsoft\internet explorer

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

agent

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\user agent

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

settings\5.0\user agent

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\user agent

Opens key: HKLM\software\wow6432node\policies

Opens key: HKCU\software\policies

Opens key: HKCU\software

Opens key: HKLM\software\wow6432node

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

settings\user agent

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

settings\user agent

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\user agent\ua tokens

 $\label{lem:constant} \mbox{ Opens key:} \qquad \mbox{ HKCU\software\mbox{microsoft\windows\currentversion\internet settings}} \\ \mbox{ Opens key:} \qquad \mbox{ HKLM\software\wow6432node\mbox{microsoft\windows\currentversion\internet}}$ 

settings\user agent\pre platform

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\user agent\pre platform

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

settings\5.0\user agent\pre platform

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\user agent\post platform

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\user agent\post platform

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

settings\5.0\user agent\post platform

Opens key: HKLM\software\wow6432node\policies\microsoft\internet

explorer\main\featurecontrol

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

Opens key: HKLM\software\wow6432node\microsoft\internet

explorer\main\featurecontrol

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

Opens key: HKLM\software\wow6432node\microsoft\internet

 $\verb|explorer| \verb|main| featurecontrol| feature\_browser\_emulation|$ 

Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid

Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype 0
Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype

O\certdllopenstoreprov
Opens key:

 $Opens~key: HKLM\software\wow6432node\microsoft\cryptography\oid\encoding type~\certdllopenstoreprov\#16$ 

Opens key: HKLM\software\wow6432node\microsoft\cryptography\oid\encodingtype

1\certdllopenstoreprov

Opens key: HKU\

Opens key: HKCU\software\microsoft\systemcertificates\my\physicalstores

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

980053277-1733835069-2361817685-1001

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

Opens key: HKCU\software\microsoft\systemcertificates\my\certificates

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer

Opens key: HKCU\software\microsoft\systemcertificates\my\crls
Opens key: HKLM\software\policies\microsoft\internet explorer

Opens key: HKLM\software\wow6432node\policies\microsoft\internet explorer\main

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

Opens key: HKLM\software\wow6432node\microsoft\rpc

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\sqmclient\windows

Opens key: HKLM\software\microsoft\sqmclient\windows

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache

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

settings\5.0\cache

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

settings\5.0\cache\content

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache\content Opens key:  $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| explorer\\| folder descriptions$ Opens kev:

33be-4251-ba85-6007caedcf9d}

Opens key:

33be-4251-ba85-6007caedcf9d}\propertybag

HKCU\software\microsoft\windows\currentversion\explorer Opens kev:

Opens key:  $HKCU \ software \ `microsoft\ `windows \ `current version \ `explorer \ `session in fo' 1 \ in the context of the context of$ 

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders

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

folders

Opens kev: HKLM\software\wow6432node\policies\microsoft\windows\explorer

Opens key: HKLM\software\policies\microsoft\windows\explorer Opens key: HKCU\software\policies\microsoft\windows\explorer

Opens key:

6fba-4fcf-9d55-7b8e7f157091}

Opens kev:

6fba-4fcf-9d55-7b8e7f157091}\propertybag

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{5e6c858f-microsoft \ windows \ current \ version \ \}$ 0e22-4760-9afe-ea3317b67173}

HKCU\software\microsoft\systemcertificates\my\ctls Opens key:

Opens key:

 ${\tt 0e22-4760-9afe-ea3317b67173} \backslash property bag$ 

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus known folders \\ ettings$ 

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

settings\5.0\cache\cookies

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens kev:

settings\5.0\cache\cookies

Opens key:

c0e9-4171-908e-08a611b84ff6}

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765dc0e9-4171-908e-08a611b84ff6}\propertybag

Opens kev:

65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag

Opens kev: HKCU\software\microsoft\systemcertificates\my\keys HKCU\software\microsoft\windows\currentversion\internet Opens kev:

settings\5.0\cache\history

HKLM\software\wow6432node\microsoft\windows\currentversion\internet Opens key:

settings\5.0\cache\history

Opens key:

b784-432e-a781-5a1130a75963}

Opens key:

b784-432e-a781-5a1130a75963}\propertybag

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

settings\5.0\cache\extensible cache

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

settings\5.0\cache\extensible cache\domstore

HKCU\software\microsoft\windows\currentversion\internet Opens kev: settings\5.0\cache\extensible cache\feedplat

Opens key:

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}$ settings\5.0\cache\extensible cache\iecompat

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

settings\5.0\cache\extensible cache\ietld  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ 

Opens key: settings\5.0\cache\extensible cache\privacie:

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset HKLM\software\wow6432node\microsoft\internet Opens key: explorer\main\featurecontrol\retry\_headeronlypost\_onconnectionreset

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_bufferbreaking\_818408

Opens key: HKLM\software\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache
 Opens key:
                         HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens key:
                         HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_allow\_long\_international\_file names|\\
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                         HKCU\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature disallow null in response headers
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
 Opens kev:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                         HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens kev:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
 Opens kev:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature use utf8 for basic auth kb967545
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens kev:
                         HKLM\svstem\currentcontrolset\control\cmf\config
 Opens key:
                         HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                         HKLM\software\wow6432node\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                         HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
 Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus appid\_catalog \setminus 0.200f744
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens kev:
Opens key:
```

Opens key:

```
Opens key:
Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
   Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 0000000000101) \ (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\00000028
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
   Opens key:
                                            HKCU\software\microsoft\windows\currentversion\internet settings\wpad
   Opens key:
                                            HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:
                                           HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
   Opens key:
                                            \label{lem:hklmsystem} \\ HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock
   Opens key:
                                            HKLM\system\currentcontrolset\services\winsock\setup migration\providers
   Opens key:
                                           HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
                                           HKCU\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                                            HKLM\software\wow6432node\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
   Opens key:
                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
                                           HKLM\software\wow6432node\microsoft\internet
  Opens kev:
explorer\main\featurecontrol\feature_http_username_password_disable
                                            HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32
   Opens kev:
                                           HKLM\software\wow6432node\microsoft\windows
   Opens key:
nt\currentversion\profilelist
   Opens key:
                                            HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
                                            HKLM\software\microsoft\sqmclient\windows\disabledsessions\
   Opens kev:
   Opens key:
                                           HKLM\software\wow6432node\microsoft\tracing\uk1822b rasmancs
   Opens key:
                                           HKLM\system\currentcontrolset\control\sqmservicelist
   Opens key:
68ad-4d8a-87bd-30b759fa33dd}
  Opens kev:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1777f761-16466432 node \ microsoft \ windows \ node \ node
68ad-4d8a-87bd-30b759fa33dd}\propertybag
   Opens key:
                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe
                                            HKLM\software\microsoft\windows
   Opens key:
nt\currentversion\appcompatflags\custom\rundll32.exe
   Opens key:
                                           HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus approximately ags
   Opens key:
                                            HKCU\software\microsoft\windows nt\currentversion\appcompatflags
                                           HKCU\software\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                                           HKLM\software\wow6432node\microsoft\internet
   Opens kev:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
   Opens key:
                                           HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
   Opens key:
                                           HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
                                            HKLM\system\currentcontrolset\services\dnscache\parameters
   Opens kev:
   Opens key:
                                            HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
   Opens key:
                                           HKLM\software\policies\microsoft\windows nt\dnsclient
   Opens key:
                                            HKLM\system\currentcontrolset\services\dns
   Opens key:
                                           HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
                                           HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
   Opens key:
   Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
   Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\
```

HKCU\software\microsoft\internet

Opens key:

```
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
                                     HKLM\software\wow6432node\microsoft\internet
  Opens kev:
explorer \verb|\main| featurecontrol| feature\_ignore\_policies\_zonemap\_if\_esc\_enabled\_kb918915
  Opens key:
HKLM \setminus software \setminus wow 6432 node \setminus policies \setminus microsoft \setminus windows \setminus current version \setminus internet
settings\zonemap\domains\
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\domains
                                     \label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
  Opens key:
settings\zonemap\domains\
  Opens kev:
settings\zonemap\ranges\
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
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\wow6432node\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:
                                     HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
                                     HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| internet|
  Opens key:
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
                                     HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\domains\
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Opens key:
settings\zonemap\domains\
  Opens key:
                                     HKLM\software\policies\microsoft\internet explorer\security
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\
  Opens kev:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
                                     HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:
  Opens key:
                                     \label{lem:hkcu} \mbox{\current} windows \mbox{\current} internet settings \mbox{\current} settings \mbox{\current} and \mbo
  Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens kev:
settings\zones
  Opens key:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
  Opens kev:
HKLM\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\0
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\0
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
                                     \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
  Opens key:
settings\zones\1
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
  Opens key:
settings\zones\1
  Opens key:
                                     HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:
                                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:
                                     HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:
                                     \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
```

```
settings\zones\4
                        HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\zones\4
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature localmachine lockdown
 Opens key:
                        HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
 Opens key:
settings\lockdown_zones\
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\0
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
 Opens key:
                        HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\1
 Opens key:
settings\lockdown_zones\1
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
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
 Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
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
                        HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\3
 Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\lockdown_zones\3
                        HKCU\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\3
 Opens key:
                        HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
 Opens kev:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
                        HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens key:
settings\lockdown_zones\4
 Opens key:
                        HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
                        HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
 Opens key:
                        HKLM\software\policies\microsoft\windows\windows error reporting
 Opens key:
                        HKLM\software\microsoft\windows\windows error reporting
 Opens key:
                        HKLM\software\microsoft\windows\windows error reporting\debug
 Opens key:
                        HKCU\software\microsoft\windows\windows error reporting
 Opens key:
                        HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
                        HKLM\software\wow6432node\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature zone elevation
 Opens key:
                        HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
                        HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| system\\| dnsclient
 Opens key:
 Opens key:
                        HKLM\software\policies\microsoft\system\dnsclient
 Opens kev:
                        HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
 Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
```

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces

Opens kev:

Opens key:

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
 Opens kev:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
 Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-
127795cce47a}
 Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-
65fee5bae0b1}
 Opens key:
                         HKLM\system\currentcontrolset\services\tcpip\linkage
 Opens key:
                         HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
 Opens key:
                         HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
                         HKLM\system\currentcontrolset\control\lsa\accessproviders
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\ldap
 Opens key:
                         HKCU\software\microsoft\internet explorer\ietld
 Opens kev:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history\microsoft.com
 Opens key:
                         HKLM\system\currentcontrolset\control\networkprovider\hworder
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\lowcache\content
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\cookies
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\lowcache\history
 Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\lowcache\extensible cache\feedplat
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\lowcache\extensible cache\iecompat
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\lowcache\extensible cache\ietld
                         HKCU\software\microsoft\windows\currentversion\internet
 Opens key:
settings\5.0\lowcache\extensible cache\privacie:
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\00f5af79-05320ef5
 Opens key:
Opens key:
                         HKCU\software\microsoft\windows\currentversion\internet
settings\connections
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
                         HKLM\system\currentcontrolset\control\session
 Oueries value:
manager[cwdillegalindllsearch]
 Queries value:
                         HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Oueries value:
                         HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value:
HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers[transparentenabled]|
                         HKLM\system\currentcontrolset\control\nls\customlocale[empty]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
 Queries value:
                         HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Oueries value:
                         HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
                         HKCU\control panel\desktop[preferreduilanguages]
 Oueries value:
                         \label{lem:hkcu} \verb|HKCU| control panel| desktop| \verb|muicached[machinepreferreduil] anguages]| \\
 Oueries value:
 Oueries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus side by side [prefer external manifest]
                         HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                         HKLM\system\setup[oobeinprogress]
 Oueries value:
 Oueries value:
                         HKLM\system\setup[systemsetupinprogress]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
 Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\shell
 Oueries value:
folders[cache]
 Oueries value:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
 Oueries value:
                         HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
```

HKLM\software\microsoft\windows

```
nt\currentversion\gre_initialize[disablemetafiles]
                          HKLM\software\wow6432node\microsoft\windows
 Oueries value:
nt\currentversion\compatibility32[83a49421cbd]
                          HKLM\software\wow6432node\microsoft\windows
 Queries value:
nt\currentversion\windows[loadappinit dlls]
 Queries value:
                          {\tt HKLM \setminus software \setminus microsoft \setminus ole[pageallocatoruse system heap]}
 Oueries value:
                          HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
 Oueries value:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
 Queries value:
                          HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations2]
                          HKLM\system\currentcontrolset\control\session
 Oueries value:
manager[pendingfilerenameoperations]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[uk1822b]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet explorer[version]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
 Queries value:
                          settings\5.0\user agent[]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[compatible]
                          Queries value:
settings\5.0\user agent[compatible]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\user agent[version]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[version]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet settings[user
agent]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\user agent[platform]
                          HKLM\software\wow6432node\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_browser_emulation[uk1822b.exe]
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation[*]
                          {\tt HKLM \backslash system \backslash current control set \backslash services \backslash crypt 32[diaglevel]}
 Oueries value:
                          HKLM\system\currentcontrolset\services\crypt32[diagmatchanymask]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 Oueries value:
980053277-1733835069-2361817685-1001[profileimagepath]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[fromcachetimeout]
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[secureprotocols]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[secureprotocols]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[secureprotocols]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[certificaterevocation]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablekeepalive]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[idnenabled]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
 Queries value:
settings[enablehttp1_1]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
 Queries value:
                          \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings[proxyhttp1.1]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[proxyhttp1.1]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
                          \label{local-condition} \mbox{HKCU\software\mbox{\sc urrentversion\sc internet}} \\
 Queries value:
settings[disablebasicoverclearchannel]
                          HKCU\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol[feature_clientauthcertfilter]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol[feature clientauthcertfilter]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
```

settings[clientauthbuiltinui]

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[syncmode5]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache[sessionstarttimedefaultdeltasecs]

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\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache\content[peruseritem]

Oueries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 caed \ folder\ ]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{352481e8-33be-4251-ba85-6007 caed \ folder \$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ fgd \ [parsing name]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ folder \ f$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ 352481e8-33be-4251-ba85-6007 caed \ ficon \ explorer \ folder \ descriptions \ folder \ fold$ 

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]

Queries value:

 $\label{thm:local-base-bound} HKLM \software \wow 6432 node \mbox{$352481e8-33be-4251-ba85-6007} caed \c following \mbox{$152481e8-33be-4251-ba85-6007} caed \c following \mbox{$152481e8-33be-4251-ba85-6007} caed \c following \mbox{$152481e8-33be-4251-ba85-6007} caed \c following \mbox{$152481e8-33be-4251-ba85-6007} caed \c following \c foll$ 

Queries value:

 $\label{thm:local-base-equal} HKLM \software \wow 6432 node \mbox{352481e8-33be-4251-ba85-6007} caed \c following \mbox{251-ba85-6007} caed \c following \mbox{251-ba85-6007} caed \c following \mbox{251-ba85-6007} caed \c following \mbox{251-ba85-6007} caed \c following \c foll$ 

Queries value:

 $\label{thm:localization} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \folder descriptions \folder \fol$ 

Queries value:

 $\label{thm:local-base-equal} HKLM \software \wow 6432 node \mbox{352481e8-33be-4251-ba85-6007} caed \c for a mable \mbox{352481e8-32be-4251-ba85-6007} and \c for a mable \c for a mable$ 

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{352481e8-33be-4251-ba85-6007 caed \ ff9d\} \ [stream]$ 

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[publishexpandedpath]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[foldertypeid]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[initfolderhandler]

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

folders[cache]

Oueries value:

 $\label{local-operator} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fit b32785-65ba-4fcf-9d55-7b8e7f157091 \category \cite{Control of the Control of the Control$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$ 

6fba-4fcf-9d55-7b8e7f157091}[parentfolder]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [description]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [relative path]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [parsing name]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [infotip]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [localized name]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [security]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream resource]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream resource type]$ 

Oueries value:

 $\label{thm:local-continuous} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fifth= 157091\fifth= 15$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [roamable]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$ 

Queries value:

 $\label{local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \fiba-24 cf-9 d55-7 b8e7 f157091 \cite{thm:beta-panded} fba-4 fcf-9 d55-7 b8e7 f157091 \cite{thm:beta-panded} fba-4 fcf-9 d55-7 b8e7 f157091 \cite{thm:beta-panded} factor \cite{thm:beta-pa$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[attributes]$ 

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[foldertypeid]}$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[initfolder handler]$ 

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

folders[local appdata]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [category]$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$ 

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder\fill\\ 626c858f-0e22-4760-9afe-ea3317b67173\folder\fill\\ 9afe-ea3317b67173\folder\fo$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (5e6c858f-0e22-4760-9afe-ea3317b67173) \ [description]$ 

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder 173\folder 173\fo$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[infotip]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{array} In construction \end{array} The substruction \en$ 

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder descriptions \currentversion\explorer\folder \currentversion\explorer\folder\fo$ 

Queries value:

 $\label{thm:local_thm:loc$ 

0e22-4760-9afe-ea3317b67173}[security]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [stream resource]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [stream resource type]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [local redirectonly]$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$ 

Oueries value:

 $\label{lem:hklm} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [publish \ expanded \ path]$ 

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [folder type id]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [initfolder \ handler]$ 

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

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache\cookies[peruseritem]

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [name]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parentfolder]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [description]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [relative path]$ 

Queries value:

 $\label{thm:local-bound} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[parsingname]} $$$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{align*.} Hklm \end{align*.} Which is a substitution and the substitution of th$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[icon]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [security]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescription\ex$ 

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \current version \explorer \folder descriptions \current \c$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [local redirectonly]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\explorer\folderdescriptions\currentversion\explorer\$ 

Queries value:

c0e9-4171-908e-08a611b84ff6}[precreate]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[stream]$ 

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot{2b0f765d-c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[attributes]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} \ [folder type id]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [initfolder \ handler]$ 

Queries value:

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

folders[cookies]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [category]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [name]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [parent folder]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [description]$ 

Oueries value:

 $\label{local-bound} HKLM \software \wow 6432 node \windows \current version \explorer \folder descriptions \current \c$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [parsing name]$ 

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [infotip]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [localized name]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [icon]$ 

Queries value:

 $\label{local-HKLM} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [stream resource]$ 

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [stream resource type]$ 

Queries value:

 $\label{lem:hamman} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[localredirectonly]$$ 

Queries value:

Queries value:

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [stream]$ 

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f$ 

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}{attributes}

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[foldertypeid]$ 

Queries value:

 $HKLM \coftware \wow6432 node \mbox{$microsoft\windows\currentversion} \explorer \folder descriptions \colored \colored$ 

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

folders[appdata]

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

settings\5.0\cache\cookies[cacheprefix]

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

settings\5.0\cache\cookies[cachelimit]

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

settings\5.0\cache\history[peruseritem]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\5.0\cache\history[peruseritem]

Queries value:

b784-432e-a781-5a1130a75963}[category]

Queries value:

b784-432e-a781-5a1130a75963}[name]

Queries value:

b784-432e-a781-5a1130a75963}[parentfolder]

Queries value:

b784-432e-a781-5a1130a75963}[description]

b784-432e-a781-5a1130a75963}[relativepath]

Queries value:

b784-432e-a781-5a1130a75963}[parsingname]

b784-432e-a781-5a1130a75963}[infotip]

Queries value:

b784-432e-a781-5a1130a75963}[localizedname]

b784-432e-a781-5a1130a75963}[icon]

b784-432e-a781-5a1130a75963}[security]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[streamresource]

b784-432e-a781-5a1130a75963}[streamresourcetype]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[localredirectonly]

Oueries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{d9dc8a3b-delta \} \\ description \setminus \{d9dc8ab-delta \} \\ descript$ b784-432e-a781-5a1130a75963}[roamable]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3bb784-432e-a781-5a1130a75963}[precreate]

Oueries value:

b784-432e-a781-5a1130a75963}[stream]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (d9dc8a3b-descriptions) \ description \ descrip$ b784-432e-a781-5a1130a75963}[publishexpandedpath]

Oueries value:

b784-432e-a781-5a1130a75963}[attributes]

b784-432e-a781-5a1130a75963}[foldertypeid]

Queries value:

b784-432e-a781-5a1130a75963}[initfolderhandler]

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

folders[history]

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

settings\5.0\cache\history[cacheprefix]

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

settings\5.0\cache\history[cachelimit]

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

settings\5.0\cache\extensible cache\domstore[cacherepair]

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

settings\5.0\cache\extensible cache\domstore[cachepath]

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

settings\5.0\cache\extensible cache\domstore[cacheprefix]

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

settings\5.0\cache\extensible cache\domstore[cachelimit]

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

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

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

settings\5.0\cache\extensible cache\feedplat[cacherepair]

```
Oueries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
   Oueries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\ietld[cacherepair]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\ietld[cachepath]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
                                                HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
   Oueries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
                                                HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
   Queries value:
settings[enableautoproxyresultcache]
   Queries value:
                                                \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} internet \end{tabular}
settings[displayscriptdownloadfailureui]
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
  Oueries value:
settings[mbcsservername]
                                                HKCU\software\policies\microsoft\windows\currentversion\internet
   Oueries value:
settings[mbcsapiforcrack]
                                                \label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu} \mbox{\tt hkcu\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu\soft\color=lem:hkcu
   Queries value:
settings[utf8servernameres]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[disableworkerthreadhibernation]
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Oueries value:
settings[disableworkerthreadhibernation]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                                                HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[socketsendbufferlength]
                                                \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Queries value:
settings[socketreceivebufferlength]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
                                                HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[maxconnectionsperserver]
   Queries value:
                                                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
                                                HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[maxconnectionsper1_0server]
   Queries value:
                                                HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet
settings[maxconnectionsper1 Oserver]
   Queries value:
                                                \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings[maxconnectionsperproxy]
                                                HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[serverinfotimeout]
   Queries value:
                                                \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
settings[connecttimeout]
   Queries value:
                                                HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[connecttimeout]
                                                HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[connectretries]
   Queries value:
                                                HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
settings[connectretries]
   Queries value:
                                                HKCU\software\microsoft\windows\currentversion\internet
```

```
settings[sendtimeout]
  Oueries value:
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
   Queries value:
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[disablentlmpreauth]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
   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} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
settings[certcachenovalidate]
                                                  \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.
   Oueries value:
settings\5.0\cache[scavengecachefilelifetime]
   Queries value:
                                                  HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache[scavengecachefilelimit]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                                                  HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[uk1822b.exe]
   Queries value:
                                                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[perusercookies]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Oueries value:
settings[dialupuselansettings]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[wpadsearchalldomains]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[bypasshttpnocachecheck]
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Queries value:
settings[bypasshttpnocachecheck]
   Queries value:
                                                  HKLM\system\currentcontrolset\control\cmf\config[system]
   Oueries value:
                                                  HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
                                                  HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[bypasssslnocachecheck]
   Queries value:
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings[enablehttptrace]
                                                  \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
   Oueries value:
settings[nocheckautodialoverride]
                                                  HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet
   Oueries value:
settings[nocheckautodialoverride]
  Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
   Queries value:
settings[dontusednsloadbalancing]
   Oueries value:
                                                  HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[mimeexclusionlistforcache]
   Queries value:
                                                  \label{lem:hkcu} \verb+KCU\+software\+microsoft\+windows\+currentversion\+internet
settings[headerexclusionlistforcache]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Oueries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
   Queries value:
                                                  \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings[dnscachetimeout]
   Queries value:
                                                  \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings[warnonpost]
                                                  HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[warnalwaysonpost]
   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} in the lemma soft \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu
settings[warnonzonecrossing]
   Queries value:
                                                  HKCU\software\microsoft\windows\currentversion\internet
```

```
settings[warnonbadcertrecving]
                                                              HKCU\software\microsoft\windows\currentversion\internet
    Oueries value:
settings[warnonpostredirect]
    Queries value:
                                                               HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
    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[warnonhttpstohttpredirect]
    Oueries value:
                                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
    Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (0000000000004 [packed catalog item]) \ details \ 
    Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000006[packedcatalogitem]
    Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (000000000007 [packed catalog item]) \ details \ d
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000009[packedcatalogitem]
    Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ (0000000000010 [packed catalog item]) \ details \ 
    Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace\_catalog 5 [serial\_access\_num]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
    Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 00000000001[library path]) \ (library path) \ (library path
    Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ (catalog\_entries \ 00000000001 \ [displaystring]
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 000000000001[providerid]
    Queries value:
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]
    Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[providerinfo]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath]
    Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000002 \ [displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
    Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000002[supported name space]]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
    Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[storesserviceclassinfo]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
    Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace \_catalog5 \ catalog\_entries \ 00000000003 [library path]
    Oueries value:
```

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

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
Oueries value:

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[librarypath] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[displaystring]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[providerid]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[addressfamily] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[enabled]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[librarypath]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerid]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[enabled]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[storesserviceclassinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerinfo]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[librarypath]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[supportednamespace]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[enabled]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[version]
 Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ catalog\_entries \ 000000000006 \ [storesserviceclassinfo] \ Queries \ value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerinfo]
 Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2\_32 numhandle buckets]$ 

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

settings\wpad[wpadoverride]

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

settings[enableautodial]

Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \setminus parameters \setminus winsock [mapping]$ 

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]

```
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
    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[nonetautodial]
                                                            HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[globaluseroffline]
                                                            HKCU\software\microsoft\windows\currentversion\internet
    Queries value:
settings[badproxyexpirestime]
    Queries value:
                                                            settings[disablebranchcache]
                                                           HKLM\software\wow6432node\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_http_username_password_disable[uk1822b.exe]
                                                           HKLM\software\wow6432node\microsoft\internet
    Queries value:
explorer\main\featurecontrol\feature_http_username_password_disable[*]
                                                           HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
    Queries value:
    Queries value:
HKLM \label{lem:hklm} LS = \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} LS = \label{lklm} LS = \label{lklm} LS = \label{lklm} LS = \label{lklm} LS = \label{lk
    Queries value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32[filetracingmask]
    Oueries value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32[enableconsoletracing]
    Queries value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32[consoletracingmask]
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32[maxfilesize]
    Oueries value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32[filedirectory]
   Oueries value:
                                                            HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
                                                           HKLM \setminus software \setminus microsoft \setminus sqmclient \setminus windows \setminus disabled processes \texttt{[12d4ea4d]]}
    Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
    Queries value:
HKLM \setminus software \setminus wow6432 \\ node \setminus microsoft \setminus tracing \setminus uk1822 \\ b\_rasmancs \\ [enable filetracing]
    Queries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus uk1822b\_rasmancs[filetracing mask]
    Queries value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b rasmancs[enableconsoletracing]
    Queries value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasmancs[consoletracingmask]
                                                           HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
    Queries value:
    Queries value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasmancs[maxfilesize]
   Oueries value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasmancs[filedirectory]
                                                            HKLM\software\policies\microsoft\windows\currentversion\internet
    Oueries value:
settings[proxysettingsperuser]
    Queries value:
                                                            HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
                                                            HKCU\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[proxyenable]
    Queries value:
                                                            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
    Queries value:
                                                            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
                                                            HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[autoconfigurl]
   Queries value:
                                                            HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
    Queries value:
                                                            HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
   Queries value:
HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} White \label{lem:hkklm} HKLM \label{lem:hkklm} White \label{
68ad-4d8a-87bd-30b759fa33dd}[category]
    Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1777f761-16466432 node \ microsoft \ windows \ node \ node
68ad-4d8a-87bd-30b759fa33dd}[name]
   Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[parentfolder]
    Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[description]
   Oueries value:
68ad-4d8a-87bd-30b759fa33dd}[relativepath]
    Oueries value:
```

68ad-4d8a-87bd-30b759fa33dd}[parsingname] Oueries value: 68ad-4d8a-87bd-30b759fa33dd}[infotip] Oueries value: 68ad-4d8a-87bd-30b759fa33dd}[localizedname] Oueries value: 68ad-4d8a-87bd-30b759fa33dd}[icon] Oueries value: 68ad-4d8a-87bd-30b759fa33dd}[security] Oueries value: 68ad-4d8a-87bd-30b759fa33dd}[streamresource] Oueries value: 68ad-4d8a-87bd-30b759fa33dd}[streamresourcetype] Queries value: 68ad-4d8a-87bd-30b759fa33dd}[localredirectonly] Oueries value: 68ad-4d8a-87bd-30b759fa33dd}[roamable] Queries value: 68ad-4d8a-87bd-30b759fa33dd}[precreate] Oueries value: 68ad-4d8a-87bd-30b759fa33dd}[stream] Queries value: 68ad-4d8a-87bd-30b759fa33dd}[publishexpandedpath] Oueries value:  $HKLM \label{lem:hklm} White the latest and the la$ 68ad-4d8a-87bd-30b759fa33dd}[attributes] Oueries value: 68ad-4d8a-87bd-30b759fa33dd}[foldertypeid] Oueries value:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1777f761-16164, 1977f761-1616, 1977f761-1616$ 68ad-4d8a-87bd-30b759fa33dd}[initfolderhandler] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[favorites] HKLM\software\microsoft\windows Queries value: nt\currentversion\appcompatflags[{d97b6486-0cfa-44d8-acc2-0f8b5941e889}] Queries value: HKCU\software\microsoft\windows  $\verb|nt\currentversion\appcompatflags[\{d97b6486-0cfa-44d8-acc2-0f8b5941e889\}]||$ Queries value: HKLM\software\microsoft\windows nt\currentversion\appcompatflags[{44480e68-dfd5-435f-bdfe-b8246fc9f90f}] HKCU\software\microsoft\windows Oueries value: nt\currentversion\appcompatflags[{44480e68-dfd5-435f-bdfe-b8246fc9f90f}] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_mime\_handling[uk1822b.exe] Queries value: HKLM\software\wow6432node\microsoft\internet explorer\main\featurecontrol\feature\_mime\_handling[\*] HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [allow unqualified query]$ HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Queries value:

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

```
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
 Oueries value:
                        HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
                        HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable dynamic update]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus topip \setminus parameters [disable reverse address registrations]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration ttl]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
                        HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Queries value:
                        HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
 Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
 Oueries value:
                        HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
 Queries value:
```

```
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[uk1822b.exe]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
 Queries value:
                          HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
                          \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\zones\0[flags]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\1[flags]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\3[flags]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\zones\4[flags]
                          HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[uk1822b.exe]
                          HKCU\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[uk1822b.exe]
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
 Oueries value:
                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[createuricachesize]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[createuricachesize]
 Queries value:
                          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[createuricachesize]
                          HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[enablepunycode]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\zonemap[autodetect]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
                          HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows
 Queries value:
nt\currentversion\compatibility32[werfault]
                          HKLM\system\currentcontrolset\control\wmi\security[5ef9ec44-fb87-4f51-
 Oueries value:
af4e-ced0840132811
                          HKLM\system\currentcontrolset\control\wmi\security[7930f74b-e328-4350-
 Queries value:
89c6-11fd93771488]
                          HKLM\software\microsoft\windows\windows error reporting[traceflags]
 Oueries value:
                          HKLM\software\microsoft\windows\windows error reporting[noreflection]
 Queries value:
                          HKCU\software\microsoft\windows\windows error reporting[noreflection]
 Oueries value:
 Queries value:
                          HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[uk1822b.exe]
                          HKLM\software\wow6432node\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_zone_elevation[*]
 Queries value:
                          {\tt HKLM \ } system \verb|\  current control set \verb|\  services \verb|\  winsock \verb|\  setup| \\
migration\providers\tcpip6[winsock 2.0 provider id]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
                          HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Queries value:
```

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[searchlist]

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [enabled \ hcp]$ 

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [registration enabled]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [register adapter name]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [domain]$ 

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\{dhcpdomain}

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\[dhcpv6domain]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip6 \setminus parameters \setminus \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \cap ameser \lor results \cap ameser \lor resu$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [names erver]$ 

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [dhcpnameserver]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [enabled \ hcp]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [registration enabled]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [register adapter name]$ 

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \interfaces \end{4.846} and \end{4.846$ 

Queries value:

Queries value:

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [dhcpnameserver]$ 

Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Oueries value:

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [queryadaptername]$ 

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [disable adapter domain name]$ 

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [registration max address count]$ 

Queries value:

Oueries value:

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [enablemulticast]$ 

Queries value:

Queries value:

 $\label{lem:hklmsystem} HKLM \system \currentcontrolset \services \tcpip\parameters \interfaces \end{subseteq} 846ee 342-7039-11 de-9d 20-806e 6f 6e 69 63 \end{subseteq} [disable adapter domain name]$ 

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enableadapterdomainnameregistration]

Queries value:

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee342-7039-11de-9d20-806e6f6e6963\} \ [registration maxaddress count]$ 

Queries value:

```
806e6f6e6963}[maxnumberofaddressestoregister]
  Oueries value:
806e6f6e6963}[enablemulticast]
                                      HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Oueries value:
  Queries value:
HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]
                                      HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Oueries value:
  Oueries value:
                                      HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
  Oueries value:
                                      HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
                                      HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
  Oueries value:
  Queries value:
                                      HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Oueries value:
                                      HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
  Oueries value:
                                      HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[privacyadvanced]
  Queries value:
                                      HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
                                      HKLM\software\wow6432node\microsoft\windows
  Queries value:
nt\currentversion\compatibility32[rundll32]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\lowcache[signature]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\lowcache\content[peruseritem]
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\5.0\lowcache\content[cacheprefix]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\content[cachelimit]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\lowcache\cookies[peruseritem]
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\5.0\lowcache\cookies[cacheprefix]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\cookies[cachelimit]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\lowcache\history[peruseritem]
                                      \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\5.0\lowcache\history[cacheprefix]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\lowcache\history[cachelimit]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\lowcache\extensible cache\feedplat[cacherepair]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\lowcache\extensible cache\feedplat[cachepath]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\lowcache\extensible cache\feedplat[cacheprefix]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\lowcache\extensible cache\feedplat[cachelimit]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\feedplat[cacheoptions]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cacherepair]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cachepath]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cacheprefix]
  Oueries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\iecompat[cachelimit]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\lowcache\extensible cache\iecompat[cacheoptions]
                                      \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{$microsoft$} \windows \current version \end{tabular} \label{thm:local_hammon_hammon} \end{tabular}
  Queries value:
settings\5.0\lowcache\extensible cache\ietld[cacherepair]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cachepath]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\lowcache\extensible cache\ietld[cacheprefix]
  Queries value:
                                      HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\lowcache\extensible cache\ietld[cachelimit]
  Queries value:
                                      \label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lem of the l
settings\5.0\lowcache\extensible cache\ietld[cacheoptions]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\lowcache\extensible cache\privacie:[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}.
```

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\privacie:[cachepath]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\privacie:[cacheprefix]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\privacie:[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\privacie:[cachelimit]
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\lowcache\extensible cache\privacie:[cacheoptions]
Queries value: HKLM\software\wow6432node\microsoft\internet

```
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[rundll32.exe]
                                       HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6]
  Oueries value:
  Sets/Creates value:
                                       HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]
  Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[1h6wzb8fyvuwzwwulyaty]
  Sets/Creates value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[14091
  Sets/Creates value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1609]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Sets/Creates value:
settings\zones\0[1406]
  Sets/Creates value:
                                       \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\lockdown_zones\1[1406]
  Sets/Creates value:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2[1406]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Sets/Creates value:
settings\lockdown_zones\3[1406]
                                      HKCU\software\microsoft\windows\currentversion\internet
  Sets/Creates value:
settings\lockdown_zones\4[1406]
                                       HKCU\software\microsoft\internet
  Sets/Creates value:
explorer\phishingfilter[shownservicedownballoon]
  Sets/Creates value:
                                      HKCU\software\microsoft\internet
explorer\recovery[clearbrowsinghistoryonexit]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Sets/Creates value:
settings[globaluseroffline]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32[enablefiletracing]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32[enableconsoletracing]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32[filetracingmask]
  Sets/Creates value:
HKLM \label{lem:hklm} LSO = LSO - 
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32[maxfilesize]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasapi32[filedirectory]
HKLM \ software \ wow 6432 node \ microsoft \ tracing \ uk 1822b\_rasmancs \ [enable file tracing]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasmancs[enableconsoletracing]
  Sets/Creates value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tracing \setminus uk1822b\_rasmancs[filetracing mask]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasmancs[consoletracingmask]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasmancs[maxfilesize]
  Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\uk1822b_rasmancs[filedirectory]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Value changes:
settings[enablehttp1_1]
  Value changes:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Value changes:
settings[warnonpost]
  Value changes:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Value changes:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
  Value changes:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1409]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Value changes:
settings\zones\1[1609]
  Value changes:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1406]
  Value changes:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1409]
  Value changes:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1609]
  Value changes:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1406]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Value changes:
settings\zones\3[1409]
  Value changes:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1609]
  Value changes:
                                       \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt internet}
settings\zones\3[1406]
                                       HKCU\software\microsoft\windows\currentversion\internet
  Value changes:
settings\zones\4[1409]
  Value changes:
                                       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1609]
  Value changes:
                                       HKCU\software\microsoft\windows\currentversion\internet
```

settings\zones\4[1406]
Value changes:

HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]

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

settings[proxyenable]

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

settings\connections[savedlegacysettings]

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

settings\zonemap[uncasintranet]

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

settings\zonemap[autodetect]

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

settings[globaluseroffline]