Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 5011, Task ID: 40060

Task ID: 40060

10

Risk Level: Date Processed: 2016-05-03 05:04:46 (UTC)

63.3 seconds Processing Time: Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\spyeye_injector.exe"

Sample ID: 5011 Type: basic Owner:

spyeye_injector.exe 2016-05-03 05:04:45 (UTC) Label: Date Added: File Type: PE32:win32:gui File Size: 103936 bytes

MD5: b98bb6d7428c3dbffcfcab2414c6daa2

SHA256 fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029

Description:

Pattern Matching Results

PE: Contains compressed section

Ocreates malicious mutex: Spyeye [Banking]

2 PE: Nonstandard section

Modifies registry autorun entries

10 Suspicious writeprocess: Spyeye [Banking]

3 Writes to a log file [Info]

Writes to memory of system processes

6 Writes to system32 folder

Packer: UPX

1 HTTP connection - response code 404 (file not found)

5 Adds autostart object

4 Reads process memory

5 Installs service

5 Abnormal sleep detected

Static Events

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

Process/Thread Events

C:\WINDOWS\Temp\spyeye_injector.exe Creates process: ["c:\windows\temp\spyeye_injector.exe"] Creates process: C:\WINDOWS\system32\wbem\wmiadap.exe [wmiadap.exe /R /T] Creates process: Reads from process: PID:1664 C:\WINDOWS\system32\calc.exe PID:1272 C:\WINDOWS\system32\svchost.exe Reads from process: PID:1972 C:\WINDOWS\explorer.exe
PID:1408 C:\WINDOWS\system32\wbem\wmiadap.exe Reads from process: Reads from process: PID:1972 C:\WINDOWS\explorer.exe Writes to process: Writes to process: PID:572 C:\WINDOWS\system32\winlogon.exe Writes to process: PID:908 C:\WINDOWS\system32\lsass.exe Writes to process: PID:1068 C:\WINDOWS\system32\svchost.exe PID:1148 C:\WINDOWS\system32\svchost.exe Writes to process: PID:1272 C:\WINDOWS\system32\svchost.exe Writes to process: Writes to process: PID:1384 C:\WINDOWS\system32\svchost.exe Writes to process: PID:1752 C:\WINDOWS\system32\spoolsv.exe PID:1960 C:\Program Files\Java\jre7\bin\jqs.exe
PID:336 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe Writes to process: Writes to process: PID:352 C:\WINDOWS\system32\ctfmon.exe Writes to process: PID:1240 C:\WINDOWS\system32\alg.exe PID:1456 C:\WINDOWS\system32\rundl132.exe PID:524 C:\WINDOWS\system32\wbem\unsecapp.exe Writes to process: Writes to process: Writes to process: Writes to process: PID:460 C:\WINDOWS\system32\wbem\wmiprvse.exe Writes to process: PID:1664 C:\WINDOWS\system32\calc.exe
PID:1408 C:\WINDOWS\system32\wbem\wmiadap.exe Writes to process: C:\WinOldFileq\83A49421643.exe

C:\WINDOWS\Temp\spyeye_injector.exe

\BaseNamedObjects\RPCController

Named Object Events

Terminates process:

Terminates process:

Creates mutex:

Cicates matex.	(baseriamedob) jeets (it econtrolle)
Creates mutex:	\BaseNamedObjects\zXeRY3a_PtW 00FFFFFF
Creates mutex:	\BaseNamedObjects\zXeRY3a_PtW 00000000
Creates mutex:	\BaseNamedObjects\K11777AQgSYeGW79751EQmMU97975IU
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!local
settings!temporary inter	net files!content.ie5!
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!cookies!
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!local
settings!history!history	.ie5!
Creates mutex:	\BaseNamedObjects\WininetConnectionMutex
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.ILH
Creates mutex:	\BaseNamedObjects\MSPMutex
Creates mutex:	\BaseNamedObjects\RAS_MO_02
Creates mutex:	\BaseNamedObjects\RAS_MO_01
Creates mutex:	\BaseNamedObjects\SHIMLIB_LOG_MUTEX
Creates mutex:	\BaseNamedObjects\ADAP_WMI_ENTRY
Creates mutex:	\BaseNamedObjects\RefreshRA_Mutex
Creates mutex:	\BaseNamedObjects\RefreshRA_Mutex_Lib
Creates mutex:	\BaseNamedObjects\RefreshRA_Mutex_Flag
Creates event:	
\BaseNamedObjects\CTF.Th	readMarshalInterfaceEvent.000000C0.00000000.00000004
Creates event:	\BaseNamedObjects\CTF.ThreadMIConnectionEvent.000000C0.00000000.00000004

\BaseNamedObjects\MSCTF.SendReceive.Event.AM.IC Creates event:

Creates event: \BaseNamedObjects\MSCTF.SendReceiveConection.Event.AM.IC \BaseNamedObjects\MSCTF.SendReceive.Event.ILH.IC Creates event:

Creates event: \BaseNamedObjects\MSCTF.SendReceiveConection.Event.ILH.IC \BaseNamedObjects\crypt32LogoffEvent Creates event:

Creates event: \BaseNamedObjects\DINPUTWINMM

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

\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1} Creates semaphore:

\BaseNamedObjects\4FBEA4B1 Creates semaphore:

Creates semaphore: \BaseNamedObjects\WMI_SysEvent_Semaphore_1272

File System Events

C:\WinOldFileq Creates: Creates: C:\WinOldFileq\

C:\WinOldFileq\83A49421643.exe Creates Creates: C:\WinOldFileq\B20776D7F8FB639

C:\WINDOWS\Prefetch\SPYEYE INJECTOR.EXE-255B270C.pf Opens:

C:\Documents and Settings\Admin Opens: Opens: C:\WINDOWS\system32\kernel32.dll

Opens:

C:\WINDOWS\system32\ntdll.dll Opens:

C:\WinOldFilea Opens:

C:\WINDOWS\system32\calc.exe Opens:

Opens: C:\WinOldFileq\

Opens: C:\WINDOWS\Temp\spyeye_injector.exe C:\WinOldFileq\83A49421643.exe Opens: Opens: C:\WINDOWS\AppPatch\sysmain.sdb C:\WINDOWS\AppPatch\systest.sdb Opens: Opens: C:\WinOldFileq\83A49421643.exe.Manifest C:\WINDOWS\Prefetch\83A49421643.EXE-1FEF9BA6.pf Opens: C:\WINDOWS\Temp\164d00e3-71a8-467f-a6a5-23bbe2515955 Opens:

C:\WINDOWS\system32\crypt32.dll Opens: Opens: C:\WINDOWS\system32\msasn1.dll Opens: C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\ws2_32.dll Opens: Opens: C:\WINDOWS\system32\ws2help.dll

C:\WINDOWS\system32\urlmon.dll.123.Manifest Opens: Opens: ${\tt C:\WINDOWS\system32\urlmon.dll.123.Config}$ C:\WINDOWS\WinSxS\x86 Microsoft.Windows.Common-Opens:

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83

C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll Opens: C:\WINDOWS\WindowsShell.Manifest

C:\WINDOWS\WindowsShell.Config Opens:

C:\WINDOWS\system32\WININET.dll.123.Manifest Opens: Opens: C:\WINDOWS\system32\WININET.dll.123.Config

Opens: C:\WINDOWS\system32\msimg32.dll
C:\WINDOWS\system32\shell32.dll Opens:

C:\WINDOWS\system32\SHELL32.dll.124.Manifest Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config Opens: Opens: C:\WINDOWS\system32\comctl32.dll

C:\WINDOWS\system32\comctl32.dll.124.Manifest Opens: C:\WINDOWS\system32\comctl32.dll.124.Config Opens: C:\WinOldFileq\B20776D7F8FB639

Opens: Opens: C:\WINDOWS\system32\user32.dll C:\WINDOWS\system32\wininet.dll Opens: C:\WINDOWS\system32\advapi32.dll Opens:

Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet

Files\Content.IE5

C:\Documents and Settings\Admin\Local Settings\History Opens:

C:\Documents and Settings\Admin\Local Settings\History\History.IE5 Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Opens:

Files\Content.IE5\index.dat

C:\Documents and Settings\Admin\Cookies Opens: C:\Documents and Settings\Admin\Cookies\index.dat Opens:

C:\Documents and Settings\Admin\Local

 ${\tt Settings\History\History.IE5\label{times.dat}}$

C:\WINDOWS\system32\mswsock.dll Opens: C:\WINDOWS\system32\hnetcfg.dll Opens: C:\WINDOWS\system32\wshtcpip.dll Opens: C:\windows\temp\spyeye_injector.exe Opens:

Opens: C:\AUTOEXEC.BAT

C:\Documents and Settings\Admin\Application Opens: Data\Microsoft\SystemCertificates\My\Certificates C:\Documents and Settings\Admin\Application

 ${\tt Data\Microsoft\SystemCertificates\My\CRLs}$

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

Data\Microsoft\SystemCertificates\My\CTLs

C:\WINDOWS\system32\MSIMTF.dll Opens: Opens: C:\WINDOWS\system32\MSCTF.dll C:\WINDOWS\system32\rasapi32.dll Opens: C:\WINDOWS\system32\rasman.dll Opens: C:\WINDOWS\system32\tapi32.dll Opens:

C:\WINDOWS\system32\TAPI32.dll.124.Manifest Opens: Opens: C:\WINDOWS\system32\TAPI32.dll.124.Config
C:\WINDOWS\system32\tapisrv.dll Opens:

Opens:

C:\Documents and Settings\All Users\Application

Data\Microsoft\Network\Connections\Pbk

Opens: ${\tt C:\WINDOWS\system32\ras}$

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

Data\Microsoft\Network\Connections\Pbk\

C:\WINDOWS\system32\sensapi.dll Opens: C:\WINDOWS\system32\rasmans.dll Opens: C:\WINDOWS\system32\winipsec.dll Opens: C:\WINDOWS\system32\rasadhlp.dll Opens: C:\WINDOWS\system32\dnsapi.dll Opens: C:\WINDOWS\system32\wbem\Logs\wbemess.log Opens:

C:\WINDOWS\system32\winrnr.dll Opens: C:\WINDOWS\system32\sens.dll Opens: C:\WINDOWS\system32\mprapi.dll Opens:

Opens: C:\WINDOWS\svstem32\activeds.dll C:\WINDOWS\system32\adsldpc.dll Opens: Opens: C:\WINDOWS\system32\samlib.dll C:\WINDOWS\system32\rastapi.dll Opens: Opens: C:\WINDOWS\system32\unimdm.tsp C:\WINDOWS\system32\uniplat.dll Opens: C:\WINDOWS\system32\kmddsp.tsp Opens: C:\WINDOWS\system32\ndptsp.tsp Opens: C:\WINDOWS\system32\ipconf.tsp C:\WINDOWS\system32\h323.tsp Opens: Opens: C:\WINDOWS\system32\h323log.txt Opens: C:\WINDOWS\system32\hidphone.tsp Opens: Opens: C:\WINDOWS\system32\hid.dll Opens: C:\WINDOWS\system32\rasppp.dll
C:\WINDOWS\system32\ntlsapi.dll Opens: C:\WINDOWS\system32\kerberos.dll Opens: Opens: C:\WINDOWS\system32\cryptdll.dll C:\WINDOWS\win.ini
C:\WINDOWS\system32\rasqec.dll Opens: Opens: C:\WINDOWS\system32\msv1_0.dll Opens: C:\WINDOWS\system32\drprov.dll Opens: C:\WINDOWS\system32\ntlanman.dll C:\WINDOWS\system32\netui0.dll Opens: Opens: C:\WINDOWS\system32\netui1.dll Opens: C:\WINDOWS\system32\netrap.dll Opens: Opens: C:\WINDOWS\system32\davclnt.dll Opens: ${\tt C:\WINDOWS\system32\wbem\Repository\$WinMgmt.CFG}$ C:\WINDOWS\system32\wbem\wmiadap.exe Opens: Opens: C:\WINDOWS\system32\apphelp.dll Opens: C:\WINDOWS\system32\wbem Opens: C · \WTNDOWS C:\WINDOWS\system32 Opens: C:\WINDOWS\system32\WBEM\WMIADAP.EXE.Manifest Opens: C:\WINDOWS\Prefetch\WMIADAP.EXE-2DF425B2.pf Opens: Opens: C:\WINDOWS\AppPatch Opens: C:\WINDOWS\Registration Opens: C:\WINDOWS\system32\config Opens: Opens: C:\WINDOWS\system32\wbem\Repository Opens: C:\WINDOWS\system32\wbem\Repository\FS C:\WINDOWS\WinSxS Opens: C:\WINDOWS\system32\unicode.nls Opens: Opens: C:\WINDOWS\system32\locale.nls Opens: C:\WINDOWS\system32\sorttbls.nls C:\WINDOWS\system32\msvcrt.dll Opens: C:\WINDOWS\system32\msvcp60.dll Opens: C:\WINDOWS\system32\rpcrt4.dll Opens: Opens: C:\WINDOWS\system32\secur32.dll C:\WINDOWS\system32\wbem\wbemcomn.dll Opens: C:\WINDOWS\system32\ole32.dll Opens: C:\WINDOWS\system32\gdi32.dll Opens: Opens: C:\WINDOWS\system32\oleaut32.dll C:\WINDOWS\system32\loadperf.dll Opens: C:\WINDOWS\system32\shimeng.dll Opens: Opens: C:\WINDOWS\AppPatch\AcGenral.dll Opens: C:\WINDOWS\system32\winmm.dll Opens: C:\WINDOWS\system32\msacm32.dll C:\WINDOWS\system32\version.dll Opens: C:\WINDOWS\system32\shlwapi.dll Opens: C:\WINDOWS\system32\userenv.dll Opens: Opens: C:\WINDOWS\system32\uxtheme.dll Opens: C:\WINDOWS\system32\ctype.nls
C:\WINDOWS\system32\sortkey.nls C:\WINDOWS\system32\rpcss.dll Opens: Opens: C:\WINDOWS\system32\winlogon.exe Opens: C:\WINDOWS\system32\xpsp2res.dll C:\WINDOWS\system32\psapi.dll Opens: C:\WINDOWS\system32\ntmarta.dll Opens: Opens: C:\WINDOWS\system32\wldap32.dll Opens: C:\WINDOWS\system32\clbcatq.dll C:\WINDOWS\system32\comres.dll Opens: Opens: C:\WINDOWS\Registration\R00000000007.clb C:\WINDOWS\system32\wbem\wbemprox.dll Opens: Opens: C:\WINDOWS\system32\wbem\wbemsvc.dll C:\WINDOWS\system32\wbem\fastprox.dll Opens: C:\WINDOWS\system32\ntdsapi.dll Opens:

C:\WINDOWS\system32\netapi32.dll Opens: Opens: C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA

C:\WTNDOWS\SYSTEM32\WBEM\PERFORMANCE\WMTAPRPL NEW.H Opens: C:\WINDOWS\SYSTEM32\WBEM\PERFORMANCE\WMIAPRPL_NEW.INI Opens:

Opens: C:\WINDOWS\system32\perfc009.dat Opens: C:\WINDOWS\system32\perfh009.dat Opens: C:\WINDOWS\SYSTEM32\CONFIG\SYSTEM C:\WINDOWS\SYSTEM32\PERFSTRINGBACKUP.TMP Opens: Opens: C:\WINDOWS\system32\PerfStringBackup.INI Opens: C:\WINDOWS\TEMP\PERFLIB_PERFDATA_E6C.DAT Opens: C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR C:\WINDOWS\TEMP\PERFLIB_PERFDATA_570.DAT Opens: Opens: C:\WINDOWS\system32\wbem\Logs\wbemcore.log C:\WINDOWS\system32\wbem\wmiprov.dll Opens: Opens: C:\WINDOWS\system32\wmi.dll

Opens: C:\WINDOWS\system32\wbem\Logs\wmiprov.log

C:0409\ Opens:

C:\WINDOWS\MUI\Fallback\0409\ Opens: C:\WINDOWS\system32\DRIVERS\MUI\0409\ Opens: Opens: C:\WINDOWS\System32\Drivers\MUI\0409\ C:\WINDOWS\system32\wbem\mofd.dll Opens: Opens: C:\WINDOWS\system32\drivers\acpi.sys Writes to C:\WinOldFileq\83A49421643.exe Writes to: C:\WinOldFilea\B20776D7F8FB639

Writes to: C:\WINDOWS\system32\wbem\Logs\wbemess.log Writes to: C:\WINDOWS\system32\wbem\Logs\wbemcore.log C:\WINDOWS\system32\wbem\Logs\wmiprov.log Writes to: Reads from: C:\WINDOWS\system32\ntdll.dll Reads from: C:\WINDOWS\system32\calc.exe C:\WINDOWS\Temp\spyeye_injector.exe C:\WinOldFileq\B20776D7F8FB639 Reads from: Reads from: C:\WINDOWS\system32\user32.dll Reads from: Reads from: C:\WINDOWS\system32\wininet.dll C:\WINDOWS\system32\ws2_32.dll C:\WINDOWS\system32\advapi32.dll C:\WinOldFileq\83A49421643.exe Reads from: Reads from: Reads from: Reads from: C:\WINDOWS\system32\crypt32.dll Reads from: C:\AUTOEXEC.BAT Reads from: C:\WINDOWS\system32\sens.dll C:\WINDOWS\win.ini Reads from: Reads from: C:\WINDOWS\system32\wbem\Repository\\$WinMgmt.CFG Reads from: C:\WINDOWS\Prefetch\WMIADAP.EXE-2DF425B2.pf C:\WINDOWS\Registration\R00000000007.clb Reads from: C:\WINDOWS\Temp\spyeye_injector.exe Deletes:

Network Events

DNS query: alexeyartemov.com DNS response alexeyartemov.com ⇒ 198.105.244.11 alexeyartemov.com ⇒ 104.239.213.7 DNS response: 88.198.13.147:443 Connects to: 198.105.244.11:80 Connects to: Connects to: 104.239.213.7:80 Sends data to: 8.8.8.8:53 88.198.13.147:443 Sends data to: Sends data to: 4.2.2.1:53 Sends data to: alexeyartemov.com:80 (198.105.244.11) Sends data to: alexeyartemov.com:80 (104.239.213.7) Receives data from: 4.2.2.1:53 Receives data from: alexeyartemov.com:80 (198.105.244.11) Receives data from: 8.8.8.8:53 Receives data from: alexeyartemov.com:80 (104.239.213.7)

Windows Registry Events

Opens key:

Opens key:

options\spyeye_injector.exe

Williaows Regis	•
Creates key:	HKCU\sessioninformation
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKCU\software\microsoft\windows\currentversion\run
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:	HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Creates key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones	\1
Creates key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones	\2
Creates key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones	/3
Creates key:	HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones	\4
Creates key:	HKCU\software\microsoft\internet explorer\phishingfilter
Creates key:	HKCU\software\microsoft\internet explorer\recovery
Creates key:	HKLM\software\classes
Creates key:	<pre>HKU\.default\software\microsoft\windows\currentversion\internet settings</pre>
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders	
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Creates key:	HKCU\software\microsoft\systemcertificates\my
Creates key:	HKCU\software\microsoft\windows nt\currentversion\winlogon
Creates key:	HKCU\software\microsoft windows
Creates key:	HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders	
Creates key:	HKLM\software\microsoft\windows\currentversion\explorer\shell folders
Creates key:	HKCU\software\microsoft\windows\currentversion\internet
settings\connections	
Creates key:	HKCU\software\microsoft\windows nt\currentversion\network\location
awareness	
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key:	HKLM\system\currentcontrolset\services\netbt\parameters
Creates key:	
HKU\.default\software\mathred{m}	icrosoft\windows\currentversion\telephony\handoffpriorities\mediamodes
Creates key:	HKLM\software\microsoft\windows\currentversion\h323tsp
Creates key:	HKLM\system\currentcontrolset\services\eventlog\application\microsoft
h.323 telephony service	provider
Creates key:	HKLM\system\currentcontrolset\control\deviceclasses
Creates key:	HKLM\software\microsoft\wbem\cimom
Creates key:	<pre>HKU\.default\software\microsoft\multimedia\audio</pre>
Creates key:	<pre>HKU\.default\software\microsoft\multimedia\audio compression manager\</pre>
Creates key:	<pre>HKU\.default\software\microsoft\multimedia\audio compression</pre>
manager\msacm	
Creates key:	<pre>HKU\.default\software\microsoft\multimedia\audio compression</pre>
manager\priority v4.00	
Creates key:	<pre>HKLM\software\microsoft\wbem\wdm</pre>
Creates key:	HKLM\system\currentcontrolset\services\sharedaccess\epoch
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]	
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]	
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]	
Deletes value:	

 $HKLM \software \microsoft \wbem \wdm[wmibinarymofresource.highdate time=29924836,low date time=41836544,name="c:\windows\system32\advapi32.dll[mofresourcename]"]$

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

HKLM\system\currentcontrolset\control\terminal server

```
Opens kev:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
    Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
     Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
                                                                   HKLM\software\microsoft\windows nt\currentversion\winlogon
     Opens key:
     Opens key:
     Opens key:
                                                                  HKLM\software\microsoft\windows nt\currentversion\diagnostics
    Opens key:
                                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\ntdll.dll
     Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\kernel32.dll
     Opens key:
                                                                   HKLM\system\currentcontrolset\control\safeboot\option
                                                                   HKLM\software\policies\microsoft\windows\safer\codeidentifiers
     Opens key:
                                                                   HKCU\software\policies\microsoft\windows\safer\codeidentifiers
     Opens key:
     Opens key:
                                                                   HKCU\
     Opens key:
                                                                   HKCU\software\policies\microsoft\control panel\desktop
     Opens key:
                                                                   HKCU\control panel\desktop
                                                                   HKLM\system\currentcontrolset\control\session manager
     Opens key:
     Opens key:
                                                                   HKLM\system\currentcontrolset\control\computername
     Opens key:
                                                                   HKLM\system\currentcontrolset\control\computername\activecomputername
     Opens key:
                                                                   HKCU\software\classes\applications\calc.exe
                                                                   HKCR\applications\calc.exe
     Opens key:
     Opens key:
                                                                   HKCU\software\microsoft\windows\shellnoroam\muicache\
     Opens key
                                                                   HKLM\system\wpa\tabletpc
     Opens key:
                                                                   HKLM\system\wpa\mediacenter
                                                                   HKLM\software\microsoft\windows nt\currentversion\appcompatflags\lavers
     Opens kev:
     Opens key:
                                                                   HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
     Opens key:
                                                                   HKLM\software\microsoft\windows
nt\current version\app compatflags\custom\83a49421643.exe
    Opens key:
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\83a49421643.exe
     Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
    Opens key
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
     Opens key:
                                                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
 options\user32.dll
Opens key: options\imm32.dll
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll
     Opens key:
                                                                   \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current + version + image + file + execution + in the content of the content + in the conten
options\crypt32.dll
     Opens key:
                                                                   HKLM\system\currentcontrolset\control\error message instrument\
     Opens key
                                                                   HKLM\system\currentcontrolset\control\error message instrument
     Opens key:
                                                                   \label{lem:hklm} \verb+KLM\software\microsoft\windows nt\currentversion\gre\_initialize\\
     Opens key:
                                                                   HKLM \  \  \, icrosoft \  \  \, int \  \  \  \, int \  
     Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\ime compatibility
     Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\windows
     Opens key
                                                                   HKLM \verb|\system| current control set \verb|\services| crypt 32 \verb|\performance| set \verb|\system| control set \|\system| control set \| control set \|\system| control 
     Opens key
                                                                   HKLM\software\microsoft\windows nt\currentversion\msasn1
     Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
     Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
    Opens key
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
     Opens key:
                                                                   HKLM\software\microsoft\windows\currentversion\explorer\performance
     Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\normaliz.dll
    Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
     Opens key:
                                                                   HKLM\software\microsoft\ole
     Opens key:
                                                                   HKCR\interface
                                                                   HKCR\interface\{00020400-0000-0000-c000-00000000046}
     Opens kev:
     Opens key:
                                                                   \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/current/version/image file execution
 options\oleaut32.dll
     Opens key:
                                                                   HKLM \verb|\software\microsoft\windows\currentversion\explorer\fileassociation
     Opens key
                                                                  HKLM\software\microsoft\oleaut
     Opens key:
                                                                   HKLM\software\microsoft\oleaut\userera
     Opens key:
                                                                   \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\iertutil.dll
    Opens key
                                                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
     Opens key:
HKLM \label{limits} \label{limits} HKLM \label{limits} KLM \label{limits} Software \label{limits} windows \label{limits} current version \label{limits} side by side \label{limits} \label{limits} as sembly storage roots
Opens key: options\comctl32.dll
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens key:
                                                                   HKCU\software\microsoft\windows\currentversion\explorer\advanced
                                                                   HKLM\software\microsoft\windows nt\currentversion\languagepack
     Opens key
     Opens key:
                                                                   \label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution
 options\wininet.dll
     Opens key:
                                                                   HKCU\software\classes\
     Opens key:
                                                                   HKCU\software\classes\protocols\name-space handler\
     Opens key:
                                                                   HKCR\protocols\name-space handler
     Opens key:
                                                                   HKCU\software\classes\protocols\name-space handler
     Opens key:
                                                                   HKCU\software\policies\microsoft\windows\currentversion\internet
 settings
     Opens key:
                                                                   HKLM\software\microsoft\windows\currentversion\internet settings
     Opens key:
                                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
settings
    Opens key:
                                                                   HKCU\software\microsoft\internet
 explorer\main\featurecontrol\feature_protocol_lockdown
     Opens key:
                                                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
    Opens key:
                                                                  HKLM\software\policies\microsoft\windows\currentversion\internet
 settings\
     Opens key:
                                                                  HKLM\software\microsoft\ctf\tip\
                                                                  HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
     Opens key:
```

```
c9633f71be64}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
                                                                                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
      Opens key
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
                                                                                           HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 80
      Opens key:
c9633f71be64}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
                                                                                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
     Opens key
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
                                                                                           HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
      Opens key
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                                          HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
      Opens key:
      Opens kev:
                                                                                           HKLM\software\microsoft\internet explorer\main\featurecontrol
       Opens key:
      Opens key:
                                                                                           \label{prop:hkcu} \begin{tabular}{ll} HKCU \software \mbox{$\stackrel{\cdot}{m}$ internet explorer \mbox{$\stackrel{\cdot}{m}$ ain}$ feature control} \end{tabular}
      Opens key:
                                                                                          {\tt HKCU \backslash software \backslash microsoft \backslash internet}
explorer\main\featurecontrol\feature ignore policies zonemap if esc enabled kb918915
                                                                                           HKLM\software\microsoft\internet
      Opens key:
\verb|explorer| main\featurecontrol\feature_ignore_policies_zonemap_if_esc\_enabled\_kb918915| \\
      Opens key:
                                                                                           \label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet
settings\zonemap\domains\
                                                                                          HKCU\software\policies\microsoft\windows\currentversion\internet
     Opens key:
settings\zonemap\domains\
                                                                                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
                                                                                          HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
     Opens key
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                                           Opens key
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
                                                                                          HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
     Opens kev:
c9633f71be64}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
      Opens key
                                                                                           HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80\} \verb|\category\item\fib5a73cd1-8355-426b-a161-259808f26b14| \\
     Opens key:
                                                                                          HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
                                                                                           HKCU\software\policies\microsoft\windows\currentversion\internet
      Opens key:
settings\zonemap\ranges\
     Opens key:
                                                                                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
                                                                                           HKLM\software\microsoft\internet
      Opens key:
explorer\main\featurecontrol\feature_unc_savedfilecheck
      Opens key:
                                                                                          HKLM\system\currentcontrolset\control\wmi\security
                                                                                           HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
      Opens key
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
      Opens key
                                                                                          HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80\} \land (c6debc0a-f2b2-4f17-930e-ca9faff4cd04) \land (c6debc0a-f2b2-4f17-95aff4cd04) \land (
     Opens key
                                                                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msimg32.dll
      Opens key:
                                                                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
      Opens key:
                                                                                           HKLM\system\setup
                                                                                           HKLM\software\microsoft\internet explorer
      Opens kev:
     Opens key:
                                                                                           \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\internet\ settings\user}} \\ \mbox{\tt windows\currentversion\simple} \\ \mbox{\tt internet\ settings\simple} \\ \mbox{\tt windows\currentversion\simple} \\ \mbox{\tt internet\ settings\simple} \\ \mbox{\tt windows\simple} \\ \mbox{\tt internet\ settings\simple} \\ \mbox{\tt windows\simple} \\ \mbox{\tt internet\ settings\simple} \\ \mbox{\tt windows\simple} \\ \mbox{\tt windows\s
agent
     Opens key
                                                                                           HKLM\software\microsoft\windows\currentversion\internet settings\user
agent
     Opens key:
                                                                                           HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
     Opens key:
                                                                                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
     Opens key:
                                                                                           HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\ua tokens
      Opens key:
                                                                                           HKCU\software\microsoft\windows\currentversion\internet settings
     Opens key:
                                                                                          HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\pre platform
      Opens key:
                                                                                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
     Opens key
                                                                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
     Opens key:
                                                                                          \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} is software \verb|\microsoft| windows \end{tabular} current version \end{tabular} internet settings \end{tabular} user \begin{tabular}{ll} \end{tabular} is software \end{tabular} in the local part of the local par
agent\post platform
      Opens key:
                                                                                           \label{lem:hklm} \verb+Kklm\+ software\+ incresoft\+ windows\+ current version\+ 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:
                                                                                          HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
                                                                                          HKLM\software\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_browser_emulation
      Opens key:
                                                                                          HKLM\system\currentcontrolset\services\winsock2\parameters
      Opens key
                                                                                          HKLM\software\policies\microsoft\internet explorer\main
      Opens key
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key
Opens key:
Opens kev:
                                                                                          HKU\.default\software\policies\microsoft\control panel\desktop
      Opens key:
                                                                                           HKU\.default\control panel\desktop
       Opens key:
                                                                                           HKCR\protocols\name-space handler\
      Opens key:
                                                                                          HKU \verb|\|.default\| software \verb|\| policies \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet | inte
settings
                                                                                          HKU\.default\software\microsoft\internet
     Opens key:
explorer\main\featurecontrol\feature_protocol_lockdown
                                                                                          HKU\.default\software\policies\microsoft\internet
      Opens key:
explorer\main\featurecontrol
      Opens key:
                                                                                           HKU\.default\software\microsoft\internet explorer\main\featurecontrol
      Opens key:
                                                                                          HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
                                                                                          HKU \verb|\|.default\| software \verb|\| policies \verb|\| microsoft\| windows \verb|\| current version \verb|\| internet | inte
settings\zonemap\ranges\
```

```
Opens kev:
                                         HKU\.default\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:
Opens key
                                         HKLM\software\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
Opens key:
                                         HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:
Opens key:
                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:
                                         {\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet}
settings\5.0\cache\cookies
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000000
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000000
  Opens key:
                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
                                         HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
\label{thm:local_catalog} HKL\begin{tabular}{ll} HKL\begin{tabular}{ll} MKL\begin{tabular}{ll} MKL\begin{tabular
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
  Opens key:
                                         HKLM\security\policy
   Opens key:
                                         HKLM\security\policy\secdesc
  Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries
  Opens key:
Opens key:
                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
                                         \label{thm:local_equation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \\
  Opens key:
settings\5.0\cache\extensible cache\domstore
  Opens key:
HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\feedplat
  Opens key:
HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\extensible cache\iecompat
                                         HKCU\software\microsoft\windows\currentversion\internet
  Opens key:
settings\5.0\cache\extensible cache\ietld
                                         HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\extensible cache\mshist012014033120140407
                                         \label{lem:hklmsoftware} \mbox{\tt HKLM\software\mbox{\tt microsoft\windows}\ nt\current version\end{\tt image} ille execution
  Opens key:
options\mswsock.dll
                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
  Opens kev:
options\hnetcfg.dll
  Opens key:
                                         HKLM\software\microsoft\rpc\securityservice
   Opens key:
                                         {\tt HKLM \ } system \verb|\  current control set \verb|\  services \verb|\  winsock \verb|\  parameters 
                                         HKCU\software\microsoft\windows\currentversion\internet
  Opens key
settings\5.0\cache\extensible cache\mshist012014041220140413
                                         {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ tcpip \verb|\ parameters \verb|\ winsock | and the substitution of the s
  Opens key:
  Opens key
                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
  Opens key:
                                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
  Opens key:
                                         HKCU\software\microsoft\internet
\verb|explorer\main\featurecontrol\retry_headeronlypost\_onconnectionreset| \\
  Opens kev:
                                         HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
                                         HKCU\software\microsoft\internet
  Opens key:
explorer \verb|\main| featurecontrol| feature\_bufferbreaking\_818408
                                         HKLM\software\microsoft\internet
  Opens key:
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:
                                         HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_skip\_post\_retry\_on\_internetwritefile\_kb895954
Opens~key: \\ HKLM \ software \ microsoft \ internet \\ explorer \ main \ feature control \ feature \ skip post retry on internet write file \ kb895954 \\
  Opens key:
                                         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
  Opens key:
                                         HKLM\software\microsoft\internet
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
```

HKLM\software\microsoft\internet

 $explorer \verb|\main| featurecontrol| feature_use_cname_for_spn_kb911149$

Opens key:

```
Opens kev:
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature use spn for ntlm auth disabled
   Opens key:
                                                HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature\_use\_spn\_for\_ntlm\_auth\_disabled| \\
   Opens key
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
   Opens key:
                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
   Opens key:
                                                HKCU\software\microsoft\internet
\verb|explorer| feature | permit_cache_for_authenticated_ftp\_kb910274| \\
                                                HKLM\software\microsoft\internet
   Opens key
\dot{\text{explorer}} \dot{\text{main}} \dot{\text{feature}} = \text{permit\_cache\_for\_authenticated\_ftp\_kb910274}
                                                HKCU\software\microsoft\internet
   Opens key:
explorer \verb|\main| featurecontrol| feature\_disable\_unicode\_handle\_closing\_callback|
                                                HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
   Opens key:
                                                HKCU\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature\_disallow\_null\_in\_response\_headers
   Opens key:
                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
   Opens key:
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
   Opens key:
                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
   Opens key:
                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
   Opens key:
                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
   Opens key:
                                                \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet settings \verb+ wpad+ \\
                                                HKCU\software\microsoft\internet
   Opens key
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
                                                HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
   Opens key:
                                                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
                                                HKLM\software\microsoft\internet
   Opens key:
explorer\main\featurecontrol\feature_http_username_password_disable
   Opens key:
                                                {\tt HKLM \ sam \ long 
                                                HKLM\sam\sam\domains\account\aliases\000003eb
   Opens key:
   Opens key:
                                                HKLM\sam\sam\domains\account\users\000003eb
                                                {\tt HKLM \backslash software \backslash microsoft \backslash cryptography \backslash oid}
   Opens key
   Opens key:
                                                HKLM \verb|\software\microsoft\cryptography\oid\encoding type 0|
   Opens kev:
                                                HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov
   Opens key:
                                                HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\#16
                                                HKLM\software\microsoft\cryptography\oid\encodingtype
   Opens key:
0\certdllopenstoreprov\ldap
                                                ...
HKLM\software\microsoft\cryptography\oid\encodingtype 1
   Opens key:
   Opens key:
                                                HKLM\software\microsoft\cryptography\oid\encodingtype
1\certdllopenstoreprov
   Opens key:
                                                HKCU\software\microsoft\systemcertificates\my\physicalstores
   Opens key:
                                                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\profilelist
                                                HKLM\system\currentcontrolset\control\session manager\environment
   Opens key:
                                                HKLM\software\microsoft\windows\currentversion
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
   Opens key
1757981266-507921405-1957994488-1003
   Opens key:
                                                HKCU\environment
   Opens key:
                                                HKCU\volatile environment
                                                HKCU\software\microsoft\systemcertificates\my
   Opens key:
   Opens key:
                                                HKCU\software\microsoft\systemcertificates\my\
   Opens key:
                                                \label{local-condition} HKCU \ software \ microsoft \ system certificates \ my \ certificates
                                                HKCU\software\microsoft\systemcertificates\my\crls
   Opens kev:
                                                HKCU\software\microsoft\systemcertificates\my\ctls
   Opens key:
   Opens key
                                                HKCU\software\microsoft\systemcertificates\my\keys
   Opens key:
                                                \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\rasman.dll
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
   Opens key:
                                                HKLM\software\microsoft\windows\currentversion\telephony
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\rasapi32.dll
   Opens key:
                                                 HKLM\software\microsoft\tracing\rasapi32
   Opens key:
                                                HKLM\system\currentcontrolset\services
   Opens key:
                                                HKLM\system\currentcontrolset\services\tapisrv
                                                HKLM\svstem\currentcontrolset\services\tapisrv\parameters
   Opens key:
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapisrv.dll
   Opens key:
                                                {\tt HKLM \backslash software \backslash microsoft \backslash tracing \backslash tapisrv}
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
options\sensapi.dll
   Opens key:
                                                HKLM\software\microsoft\com3
   Opens key:
                                                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}
                                                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\treatas
   Opens key
   Opens key:
                                                HKCR \verb|\clsid|{d5978620-5b9f-11d1-8dd2-00aa004abd5e} \verb|\inprocserver32| \\
   Opens key:
   Opens key:
                                                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\label{line} \label{line} In proceser verx 86
                                                \label{localserver32} $HKCR\clsid_{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\longrightarrow HCR\clsid_{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\longrightarrow HCR\clsid_{d5978620-
   Opens key:
   Opens key:
                                                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprochandlerx86
   Opens key:
                                                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\localserver
   Opens key:
   Opens key:
                                                HKCR\appid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}
                                                HKCU\software\microsoft\windows\currentversion\internet settings\http
   Opens kev:
filters\rpa
   Opens key:
                                                HKLM\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
   Opens key:
                                                HKCU\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature include port in spn kb908209
                                                           HKLM\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
                                                           HKCU\software\microsoft\internet
    Opens key:
explorer\main\featurecontrol\feature_mime_handling
                                                           HKLM\software\microsoft\internet
    Opens key:
 explorer\main\featurecontrol\feature mime handling
                                                            HKLM\system\currentcontrolset\control\productoptions
     Opens key:
    Opens key:
                                                           HKLM\software\policies\microsoft\system\dnsclient
    Opens key:
                                                            HKLM\system\currentcontrolset\services\tcpip\parameters
                                                            HKLM\software\microsoft\windows\currentversion\telephony\server
    Opens kev:
                                                            HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
     Opens key:
    Opens key:
                                                            \label{locality} HKCR \verb|\clsid|{1be1f766-5536-11d1-b726-00c04fb926af}\\ \verb|\treatas|
    Opens key:
                                                            HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprocserver32
                                                            HKLM\system\currentcontrolset\services\rasman
    Opens key:
                                                            HKLM\system\currentcontrolset\services\rasman\parameters
     Opens key:
    Opens key:
                                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\winipsec.dll
    Opens key:
                                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\rasmans.dll
                                                            Opens key:
                                                           HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\localserver32
HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler32
    Opens key:
    Opens key:
    Opens key:
                                                            HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandlerx86
                                                            HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\localserver
     Opens key:
                                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options \\ \\ \hat{rasadhlp.dll}
                                                            HKCU\software\microsoft\windows\currentversion\internet
    Opens kev:
 settings\zonemap\
    Opens key:
                                                            HKLM\software\policies\microsoft\internet explorer\security
                                                           HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}
HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\treatas
     Opens key:
    Opens key:
                                                            HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32
    Opens key:
     Opens key:
                                                            HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}
    Opens key:
                                                            \label{lem:hkcu} \mbox{HKCU\software\mbox{\sc urrentversion\internet settings\sc varies} \mbox{\sc urrentversion\sc urrentversion\sc varies} \mbox{\sc urrentversion\sc u
                                                            HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserverx86
    Opens kev:
                                                            HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\localserver32
    Opens key:
                                                            HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprochandler32
     Opens key:
    Opens key:
                                                            HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\dnsapi.dll
    Opens key:
                                                            HKLM\system\currentcontrolset\services\dnscache\parameters
     Opens key:
                                                            HKLM\software\policies\microsoft\windows nt\dnsclient
     Opens key:
                                                            \label{localization} HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\\\ \label{localization} \\ \label{localization} IRCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\\\ \label{localization} \\ \label{localization} HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\\\ \label{localization} \\ \label{localization} HKCR\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\clsid\cl
    Opens key:
                                                            \label{localserver} HKCR \ clsid \ \{5b035261-40f9-11d1-aaec-00805fc1270e\} \ \ localserver
                                                            HKLM\svstem\currentcontrolset\control\network
    Opens kev:
                                                            HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
    Opens key
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}
Opens key: \label{lem:hkklmsystem} HKLM \system \currentcontrolset \colored by the control of 
                                                           HKU\.default\software\microsoft\windows\shellnoroam\muicache\
    Opens key:
    Opens key:
                                                            08002be10318\} \setminus \{b7d3b707-8bc4-489e-84f0-d92eb38c0674\} \setminus interfaces
    Opens key:
                                                           HKU\s-1-5-18 classes
    Opens key:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
 c7d49d7cecdc}
    Opens key:
                                                            HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}
                                                            HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\treatas
    Opens kev:
    Opens key:
                                                            HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprocserver32
     Opens key:
                                                            HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprocserverx86
    Opens key:
                                                            HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\localserver32
    Opens key:
                                                            HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}
                                                            HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\treatas
    Opens key:
                                                            HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprocserver32
     Opens key:
    Opens key:
                                                            \label{local-condition} HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\\\ \\\ inprochandler 32
    Opens key:
                                                            \label{localization} \begin{tabular}{ll} HKCR\clsid\\ a907657f-6fdf-11d0-8efb-00c04fd912b2\\ \end{tabular} \begin{tabular}{ll} \begin{tabular}{ll} A907657f-6fdf-11d0-8efb-00c04fd912b2\\ \end{tabular} \begin{tabular}{ll} \begin{
                                                            HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\localserver
    Opens kev:
                                                            HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprocserverx86
    Opens key:
    Opens key:
                                                            HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\localserver32
     Opens key:
                                                           HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprochandler32
HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprochandlerx86
    Opens key:
    Opens key:
                                                            HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\localserver
     Opens key:
                                                            HKLM\system\currentcontrolset\services\eventlog\system
    Opens key:
                                                            HKLM\system\currentcontrolset\services\eventlog\system\service control
manager
    Opens key
                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001
    Opens key:
                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi
    Opens kev:
                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 08002be10318}\0001\ndi\interfaces
                                                            HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
    Opens key
Opens key:
08002be10318}\0008
                                                           HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
    Opens key:
                                                            HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi
Opens key: HKLM\sys 08002be10318}\0008\ndi\interfaces
                                                            Opens key:
                                                            HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\treatas
                                                            HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32
     Opens key
     Opens key:
                                                            HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\label{eq:hkcr} \label{eq:hkcr} In processor \end{array} \label{eq:hkcr}
    Opens key
                                                            HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\localserver32
                                                            HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler32
    Opens key:
                                                            HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandlerx86
     Opens key:
                                                            HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\localserver
     Opens key
Opens key:
                                                            HKLM\system\currentcontrolset\services\tcpip
    Opens key
                                                            HKLM\system\currentcontrolset\services\tcpip\parameters\adapters
    Opens key
```

```
HKLM\svstem\currentcontrolset\services\tcpip\parameters\adapters\ndiswanip
                  HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
 Opens key:
 Opens key:
                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winrnr.dll
                  HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib
 Opens key:
                 HKCR\typelib
 Opens key:
                  HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}
 Opens key:
 Opens key:
                  HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0
 Opens key:
                 HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0
                 Opens key:
 Opens kev:
HKLM\system\currentcontrolset\services\dhcp\configurations\alternate {16325b0b-4636-4303-abe3-
c7d49d7cecdc}
Opens key: HKLM\system\currentcontrols 08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}
                 HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
 Opens key:
                 HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}
                 HKLM\system\currentcontrol\set\control\network\{4d36e975-e325-11ce-bfc1-
 Opens key
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi
Opens~key: \\ HKLM\system\currentcontrolset\control\ntwo 88002be10318\\ \{61eab4e1-adba-45df-86af-11c0d7f92321\}\ndi\interfaces
                 Opens key:
                 HKLM\system\currentcontrolset\services\vxd\mstcp
 Opens key:
                 HKLM\system\currentcontrolset\control\computername\computername
                 HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
 Opens key:
Opens key:
                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\adsldpc.dll
 Opens key:
                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\activeds.dll
 Opens key:
                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\samlib.dll
 Opens key:
                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\mprapi.dll
 Opens key:
                  HKLM\system\currentcontrolset\services\netbt
 Opens key:
                  {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ net bt \verb|\ parameters \verb|\ interfaces | \\
 Opens key:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{16325b0b-4636-4303-
abe3-c7d49d7cecdc}
 Opens key:
                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rastapi.dll
 Opens key:
                 HKLM\software\microsoft\tracing\rastapi
                 HKLM\software\microsoft\eventsvstem\{26c409cc-ae86-11d1-b616-
 Opens key
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
 Opens key
00805fc79216}\subscriptions\{6b9c1fb5-c711-47f3-94f9-bac5ad5535fe}-{00000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\tracing\tapi32
 Opens key:
                  HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616
Opens key
Opens key:
                  HKLM \verb|\software\microsoft\windows\currentversion\telephony\providers
 Opens key:
                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uniplat.dll
 Opens key:
                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\unimdm.tsp
Opens key:
options\kmddsp.tsp
                  HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
                  HKLM\software\microsoft\tracing\kmddsp
 Opens key
                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ndptsp.tsp
                 \label{thm:hklm:software} $$HKLM\software\microsoft\windows nt\currentversion\image file execution $$ $$ $$
 Opens key
 Opens key:
options\ipconf.tsp
 Opens key:
                  HKLM\software\microsoft\tracing\conftsp
Opens key:
options\h323.tsp
                  HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key:
                  HKLM\system\currentcontrolset\services\eventlog\application
                  HKLM\software\microsoft\windows nt\currentversion\image file execution
 Opens key
options\hid.dll
 Opens key
                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hidphone.tsp
 Opens key:
                  HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
88cb-001111000030}
 Opens key:
                  HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
```

```
08002he103183
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key
08002be10318}\0000
   Opens key:
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key
08002be10318}\0003
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key:
08002be10318}\0004
   Opens key:
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005
   Opens key:
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006
   Opens key:
                                             HKLM\svstem\currentcontrolset\services\remoteaccess
                                             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
   Opens key
08002be10318}\0007
   Opens key
                                             HKLM\system\currentcontrolset\services\nbf\linkage
Opens key:
options\ntlsapi.dll
                                             \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
   Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasppp.dll
   Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cryptdll.dll
   Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kerberos.dll
                                             HKLM\system\currentcontrolset\services\rasman\parameters\quarantine
   Opens key
   Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasgec.dll
   Opens key:
                                             HKLM\software\microsoft\tracing\rasqec
   Opens key
                                             HKLM\software\microsoft\tracing\rasm
   Opens key:
                                             {\tt HKLM \ } software \ \\ microsoft \ \\ tracing \ \\ ppp
                                             HKLM\software\microsoft\tracing\bap
   Opens key:
   Opens key:
                                             HKLM\system\currentcontrolset\services\rasman\ppp
   Opens key
                                             HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols
   Opens key
{\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ rasman \verb|\ ppp \verb|\ control protocols \verb|\ builtin 
                                             HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\chap
   Opens key:
                                             HKLM\software\microsoft\tracing\rasspap
   Opens key:
   Opens key:
                                             HKLM\system\currentcontrolset\services\rasman\ppp\spap
   Opens key:
                                             HKLM\software\microsoft\tracing\raspap
   Opens key:
                                             HKLM\software\microsoft\tracing\raseap
   Opens key:
                                             HKLM\system\currentcontrolset\services\rasman\ppp\eap
   Opens key:
                                             HKLM\system\currentcontrolset\services\rasman\ppp\eap\13
   Opens key:
                                             HKLM \verb|\system| current control set \verb|\services| rasman \verb|\ppp| eap \verb|\25| 
                                             HKLM\system\currentcontrolset\services\rasman\ppp\eap\26
   Opens kev:
   Opens key:
                                             HKLM\system\currentcontrolset\services\rasman\ppp\eap\4
                                             HKLM\software\microsoft\tracing\rasccp
   Opens key:
   Opens key:
                                             HKLM\software\microsoft\tracing\rasbacp
                                             HKLM\software\microsoft\tracing\rasiphlp
HKLM\system\currentcontrol\securityproviders
   Opens key:
   Opens kev:
   Opens key:
                                             HKLM\system\currentcontrolset\control\lsa\sspicache
   Opens key:
                                             Opens key:
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll
                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
   Opens key:
   Opens key:
                                             HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
   Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msv1 0.dll
   Opens key:
                                             HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip
   Opens key:
\label{thm:local_hklm} \begin{tabular}{ll} HKLM \end{tabular} which is a parameter shifted by the statement of the statemen
fb0d4cf73262}
   Opens key:
                                             HKLM\system\currentcontrolset\services\netbt\parameters
   Opens key:
82c4-fb0d4cf73262}
Opens key: 
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}
   Opens key:
Opens key:
                                             HKLM\software\microsoft\tracing\rasipcp
   Opens key:
                                             \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\mpr.dll
   Opens key:
                                             HKLM\system\currentcontrolset\control\networkprovider\hworder
   Opens key:
                                             HKLM\system\currentcontrolset
                                             HKLM\system\currentcontrolset\services\rdpnp\networkprovider
   Opens key:
   Opens key:
                                             HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider
   Opens key:
                                             HKLM\system\currentcontrolset\services\webclient\networkprovider
   Opens kev:
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\drprov.dll
                                             \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current + version + image + file + execution + in the content of the content + in the conten
   Opens key:
options\netui0.dll
   Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\network\world full
access shared parameters
   Opens key:
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netrap.dll
Opens key: options\netui1.dll
                                             HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
                                             \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\ntlanman.dll
Opens key:
options\davclnt.dll
                                             \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
   Opens key:
                                             HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}
   Opens key:
   Opens key:
                                             HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\treatas
                                             HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprocserver32
   Opens key:
   Opens key:
                                             HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\nprocserverx86
   Opens key:
                                             HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\localserver32
   Opens key:
                                             HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprochandler32
                                             HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\)\ in prochandler x86
   Opens key:
```

```
Opens kev:
                                                                 HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\localserver
    Opens key:
                                                                 HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}
    Opens key:
                                                                 HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\treatas
                                                                 Opens key:
    Opens key:
                                                                 HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprocserverx86
                                                                 HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\localserver32
    Opens key:
                                                                 HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprochandler32
    Opens key:
                                                                 HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprochandlerx86
     Opens key:
    Opens key:
                                                                 HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\localserver
    Opens key:
                                                                 HKLM\system\currentcontrolset\control\minint
                                                                 HKLM\svstem\currentcontrolset\control\session manager\appcertdlls
    Opens kev:
     Opens key:
                                                                 HKLM\system\currentcontrolset\control\session manager\appcompatibility
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
{\tt options \ \ lapphelp.dll}
                                                                 HKU\.default\software\microsoft\windows
    Opens key:
nt\currentversion\appcompatflags\layers
    Opens key:
                                                                 HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\wmiadap.exe
                                                                 HKLM\software\microsoft\windows nt\currentversion\appcompatflags
    Opens key:
                                                                 HKCU\software\microsoft\windows nt\currentversion\appcompatflags
    Opens key:
    Opens key:
                                                                 HKU \verb|\|.default\| software \verb|\| microsoft\| windows | nt\| current version \verb|\| app compatflags | nt\| current version | nt\| current 
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wmiadap.exe
    Opens key:
                                                                 HKCU\appevents\schemes\apps\.default\systemnotification\.current
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acgenral.dll
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp60.dll
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemcomn.dll
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\loadperf.dll
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.dll
    Opens key:
                                                                 \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\winmm.dll
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
    Opens key:
                                                                 HKU\.default\control panel\international
    Opens key:
                                                                 HKLM\system\currentcontrolset\control\nls\locale
     Opens key:
                                                                 HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
    Opens key:
                                                                 HKLM\system\currentcontrolset\control\nls\language groups
    Opens key:
                                                                 HKLM\software\microsoft\rpc\pagedbuffers
                                                                 HKLM\software\microsoft\rpc
    Opens kev:
    Opens key:
                                                                 \label{lem:hklm} \mbox{HKLM} \mbox{$\stackrel{\cdot}{\sc hklm}$ indows nt\current version\sc file execution} \\
options\wmiadap.exe\rpcthreadpoolthrottle
                                                                 HKLM\software\policies\microsoft\windows nt\rpc
    Opens key:
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32
    Opens key:
Opens key:
                                                                 {\tt HKLM \backslash software \backslash microsoft \backslash audio compression manager \backslash driver cache}
    Opens key
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.ima adpcm
     Opens key:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msadpcm
    Opens key:
                                                                 HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
    Opens key:
Opens key:
    Opens key:
                                                                 HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
    Opens kev:
HKLM \label{limits} \begin{tabular}{ll} HKLM \label{limits} Software \end{tabular} icrosoft \label{limits} audio compression manager \end{tabular} driver cache \end{tabular} icrosoft \label{limits} audio compression manager \end{tabular} audio 
    Opens key:
\label{local-operator} \begin{tabular}{ll} HKLM \end{tabular} $$\operatorname{LMLM} \end{tabular} is $$\operatorname{LMLM} \end{tabular} $$\operatorname{LMLM} \
    Opens key:
    Opens key:
                                                                 HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm
     Opens key:
                                                                 {\it HKLM} \verb|\system| current controlset| control| mediare sources| acm
    Opens key:
                                                                 HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| explorer \verb|\| advanced | large explorer | la
    Opens key:
                                                                 HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
    Opens key:
                                                                 HKLM\software\policies\microsoft\windows\system
    Opens key:
                                                                 HKU\.default\software\microsoft\windows\currentversion\thememanager
    Opens key:
                                                                 HKLM\system\currentcontrolset\control\lsa
    Opens kev:
                                                                 HKLM\software\microsoft\wbem\cimom
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll
    Opens key:
                                                                 HKLM\system\currentcontrolset\services\ldap
    Opens key:
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntmarta.dll
    Opens key:
                                                                 \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\comres.dll
Opens key: options\clbcatq.dll
                                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
                                                                 HKLM\software\microsoft\com3\debug
                                                                 HKLM\software\classes
     Opens key:
    Opens key:
                                                                 HKU\
                                                                 HKCR\clsid
    Opens key:
    Opens key:
                                                                 HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
     Opens key:
                                                                 HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
    Opens key:
                                                                 HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32
                                                                 HKCR \verb|\clsid| \{4590f811-1d3a-11d0-891f-00aa004b2e24\} \verb|\inprocserverx86|
    Opens key:
```

```
Opens key:
                                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver32
                                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32
   Opens key:
   Opens key:
                                          HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86
                                           HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver
   Opens key:
   Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemprox.dll
                                          HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
   Opens key:
   Opens key:
                                          HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
   Opens key:
                                          Opens key:
                                          HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserverx86
                                          HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver32
   Opens kev:
   Opens key:
                                           HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler32
                                          Opens key
   Opens key:
                                          HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver
                                          HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
   Opens key:
                                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
   Opens key:
   Opens key:
                                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas
                                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86
   Opens key:
   Opens key:
                                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32
   Opens key:
                                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32
   Opens key:
                                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandlerx86
   Opens key
                                          HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver
   Opens key:
                                          HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
   Opens key:
                                          HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32
   Opens key:
   Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemsvc.dll
                                          HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
   Opens kev:
   Opens key:
                                          HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32
   Opens key
                                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
   Opens key:
                                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
                                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32
   Opens key:
                                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserverx86
   Opens key:
                                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver32
   Opens key
   Opens key:
                                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\tinprochandler 32abber \label{eq:hkcr}
                                          \label{local-condition} {\tt HKCR\clsid\d68af00a-29cb-43fa-8504-ce99a996d9ea}\ \ in prochandler x 86
   Opens kev:
                                          HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver
   Opens key:
                                          HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
   Opens key:
   Opens key:
                                          Opens key:
                                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\netapi32.dll
   Opens key:
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdsapi.dll
Opens key:
options\fastprox.dll
                                          HKLM\software\microsoft\windows nt\currentversion\image file execution
                                          HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}
   Opens key:
                                          HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\treatas
   Opens key:
   Opens key:
                                          \label{locality} HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\\\\\\\\\\\\\\\
   Opens key:
                                          HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\inprocserverx86
                                          HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\localserver32
   Opens kev:
   Opens key:
                                          \label{local-bound} HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\\\\\\\\\\\\\\\\\\\\\
   Opens key:
                                          \label{local-bound} HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\\\\) in prochandler x 86
   Opens key:
                                          HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\localserver
                                          HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}
   Opens key:
   Opens key:
                                          HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\treatas
   Opens key:
                                          HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\inprocserver32
   Opens key:
                                          HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\ \ \ in procserver x 86
                                          HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\localserver32
   Opens key:
                                          HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\inprochandler32
   Opens key:
                                           HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\inprochandlerx86
   Opens key:
   Opens key:
                                          HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}\localserver
   Opens key:
                                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
                                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas
   Opens key:
                                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32
   Opens key:
                                          \label{local-bound} HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\ \ inprocserverx86
   Opens key
   Opens key:
                                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver32
                                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32
   Opens kev:
   Opens key:
                                          Opens key:
                                          HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserve
                                          HKCR\interface\{027947e1-d731-11ce-a357-00000000001}
HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32
   Opens key:
   Opens key:
   Opens key:
                                          HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
                                          \label{localization} \mbox{HKCR\interface} $$ HKCR \inf {1c1c45ee-4395-11d2-b60b-00104b703efd} \rightarrow \mbox{Proxystubclsid32} $$ \mbox{HKCR\subseteq} $$ \mb
   Opens key:
                                          HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}
HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\treatas
   Opens key:
   Opens key:
                                          HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\inprocserver32
   Opens key:
                                           HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\inprocserverx86
   Opens key:
   Opens key:
                                          HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\localserver32
   Opens key:
                                          HKCR \verb|\clsid|{cc9072ab-c000-49d8-a5aa-00266c8dbb9b} \verb|\inprochandler32| and the state of the 
                                          HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\inprochandlerx86
   Opens kev:
   Opens key:
                                          HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\localserver
                                          HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
   Opens key
   Opens key:
                                          HKCR \verb|\interface| \{423ec01e-2e35-11d2-b604-00104b703efd\} \verb|\proxystubclsid32| 
                                          HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}
   Opens key:
                                          HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\inprocserver32
   Opens key:
   Opens key:
                                          HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\localserver32
   Opens key:
                                          HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}
   Opens kev:
                                          HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\treatas
   Opens key:
                                          HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\inprocserver32
   Opens key:
                                          HKCR\clsid\\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\\{inprocserverx86}
   Opens key:
                                          \label{localserver32} HKCR\clsid\\ \{eac8a024-21e2-4523-ad73-a71a0aa2f56a\\ \}\\ \localserver32
                                          \label{local-equation} $HKCR\clsid\\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\\inprochandler32$$HKCR\clsid\\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\\inprochandlerx86$$
   Opens key:
   Opens key:
                                          HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\localserver
   Opens key:
                                          HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
   Opens key:
   Opens key:
                                          HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas
                                          HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32
   Opens kev:
   Opens key:
                                          HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\label{eq:hkcr} \label{eq:hkcr} IRCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\label{eq:hkcr} \label{eq:hkcr}
   Opens key:
                                          HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\localserver32
   Opens key:
                                          HKCR \verb|\clsid|{674b6698-ee92-11d0-ad71-00c04fd8fdff}\\ \\ inprochandler 32 \\ \\
   Opens key:
                                          HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprochandlerx86
```

```
HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\implemented
   Opens key:
categories\{00000003-0000-0000-c000-000000000046}
                                                HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}
   Opens key:
                                                HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\treatas
                                                HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprocserver32
   Opens key:
   Opens key:
                                                HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86
   Opens key:
                                                HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\localserver32
   Opens key:
                                                HKCR \ clsid \ \{4590f812-1d3a-11d0-891f-00aa004b2e24\} \ \ in prochandler 32
                                                HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86
   Opens key:
                                                HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\localserver
   Opens kev:
                                                 HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\treatas
   Opens key:
   Opens key:
                                                Opens key:
                                                HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\ \ \ in prochandler 32
                                                HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\inprochandlerx86
   Opens key:
                                                HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\localserver
   Opens key:
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wmiprov.dll
   Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wmi.dll
   Opens key:
                                                HKLM\software\microsoft\wbem\wdm
   Opens key:
                                                HKLM\system\currentcontrolset\control\nls\muilanguages
   Opens key:
                                                HKLM\system\currentcontrolset\services\acpi
   Opens key:
                                                HKLM\system\currentcontrolset\services\mssmbios
   Opens key:
                                                 HKLM\system\currentcontrolset\services\pcnet
   Opens key:
                                                HKLM\system\currentcontrolset\services\ipnat
   Opens key:
                                                HKLM\system\currentcontrolset\services\http
                                                HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}
   Opens kev:
                                                HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\treatas
   Opens key:
   Opens key
                                                HKCR \verb|\clsid| \{c10b4771-4da0-11d2-a2f5-00c04f86fb7d\} \verb|\inprocserver32| \\
                                                HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\inprocserverx86
HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\localserver32
   Opens key:
   Opens key:
                                                HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\inprochandler32
   Opens key:
   Opens key:
                                                \label{local-equation-of-HKCR} HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\\\ \label{local-equation-of-higher-equation} In prochamble \{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\
   Opens key:
                                                Opens key:
                                                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mofd.dll
   Opens key:
                                                 HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}
   Opens key:
                                                HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\ \ treat as
   Opens key
                                                HKCR \verb|\clsid|{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\\ \\ inprocserver 32
                                                HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\inprocserverx86
   Opens key:
                                                HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\localserver32
   Opens key:
   Opens key:
                                                HKCR \verb|\clsid|{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\\ \\ inprochandler 32 \\ \\
   Opens key:
                                                \label{locality} HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\inprochandlerx86\ HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\localserver
   Opens kev:
                                                HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\implemented
   Opens key:
categories\{00000003-0000-0000-c000-000000000046}
   Queries value:
                                                HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
                                                HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
   Queries value:
   Queries value:
   Queries value:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers [transparent enabled]
   Oueries value:
                                                HKCU\control panel\desktop[multiuilanguageid]
                                                HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
   Queries value:
   Queries value:
\label{thm:local_computername} \label{thm:local_computername} \\ \text{HKLM} \\ \text{System} \\ \text{currentcontrolset} \\ \text{control} \\ \text{computername} \\ \text{putername} \\
   Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
   Queries value:
                                                HKLM\system\wpa\mediacenter[installed]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
   Queries value:
                                                HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                                                HKLM\software\microsoft\windows
nt\currentversion\compatibility32[83a49421643]
   Oueries value:
                                                HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[83a49421643]
   Queries value:
                                                HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
   Queries value:
                                                HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
                                                HKLM\software\microsoft\ole[rwlockresourcetimeout]
   Queries value:
                                                HKCR\interface[interfacehelperdisableall]
   Queries value:
                                                HKCR\interface[interfacehelperdisableallforole32]
   Queries value:
                                                HKCR\interface[interfacehelperdisabletypelib] HKCR\interface\{00020400-0000-0000-c000-
   Queries value:
   Oueries value:
00000000046}[interfacehelperdisableall]
                                                HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableallforole32]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
   Queries value:
                                                HKCU\control panel\desktop[smoothscroll]
   Queries value:
HKLM\software\microsoft\windows\currentversion\internet
   Oueries value:
settings[disableimprovedzonecheck]
   Queries value:
                                                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[83a49421643.exe]
   Oueries value:
                                                HKIM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
                                                HKLM \setminus software \setminus icrosoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}[dword]
\label{lem:queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-77e8f3d1aa80}\category\tem\{34745c63-b2f0-4784-8b67-5e12c8701a31\}[dword]}
                                                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
   Queries value:
77e8f3d1aa80\} \\ category \\ item \\ \{5130a009-5540-4fcf-97eb-aad33fc0ee09\} \\ [dword]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb500e-26ed-4fcc-854c-77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[dword]
   Queries value:
                                                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\i
                                               tem\{b5a73cd1-8355-426b-a161-259808f26b14}[dword]
   Queries value
                                                HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb1
```

HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\localserver

Opens key:

```
Oueries value:
                                             HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[dword]
   Queries value:
                                             0000-00000000000001
   Queries value:
                                             HKLM\system\setup[systemsetupinprogress]
   Oueries value:
                                             HKLM\software\microsoft\internet explorer[version]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\user agent[]
   Queries value:
                                             HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\user agent[compatible]
                                             HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\user agent[compatible]
  Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
   Queries value:
                                             HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet settings[user
agent]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
  Oueries value:
                                             HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [winsock\_registry\_version]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
   Queries value:
                                             HKLM\software\policies\microsoft\internet
explorer\main[security hklm only]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevo
  Queries value:
                                             \label{thm:local_thm:local_thm} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet}} \\
settings[disablekeepalive]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[disablepassport]
   Queries value:
                                             \label{thm:local_equation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt local_equation} \mbox{\tt local_equation} \mbox{\tt local_equation}} \mbox{\tt local_equation} \mbox{\tt local_
settings[idnenabled]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
   Queries value
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
                                             HKCU\software\microsoft\internet
   Queries value:
\verb|explorer\main\featurecontrol[feature\_clientauthcertfilter]| \\
   Oueries value
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[num catalog entries]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings[clientauthbuiltinui]
                                             HKU\.default\control panel\desktop[multiuilanguageid]
   Queries value:
   Queries value
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[lsass.exe]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
   Queries value:
                                             HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
  Queries value:
                                             \label{thm:local_equation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \\
settings\5.0\cache[signature]
  Queries value:
                                             \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ internet
settings\5.0\cache\content[peruseritem]
   Queries value:
Queries value:
HKLM \ system \ current controls et \ services \ \ winsock 2 \ parameters \ \ protocol\_catalog9 \ \ catalog\_entries \ \ \ 0000000000003 \ [packed catalogitem]
   Oueries value:
HKLM \\ system \\ current control set \\ services \\ winsock \\ a parameter \\ sprotocol\_catalog \\ o catalog\_entries \\ 00000000000000000[packed catalog item] \\ determines \\ deter
   Queries value:
                                             HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:
HKL\\ Mxystem\\ current controlset\\ services\\ winsock2\\ parameters\\ protocol\_catalog9\\ catalog\_entries\\ 0000000000005[packed catalogitem]
   Queries value:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[calc.exe]
   Oueries 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:
                                             \label{lem:hkcu} \verb+KKCU \+ software \+ microsoft \+ windows \+ current version \+ internet
settings\5.0\cache\cookies[peruseritem]
                                             HKLM\software\microsoft\windows\currentversion\internet
   Oueries value:
settings\5.0\cache\cookies[peruseritem]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000007[packedcatalogitem]
```

```
Oueries value:
Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
  Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
                                          HKLM\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\history[peruseritem]
  Queries value:
                                          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
  Oueries value:
Queries value:
Oueries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
  Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
                                          HKLM\security\policy\secdesc[]
  Queries value:
  Queries value:
Oueries value:
Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ [num\_catalog\_entries]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[displaystring]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000001[enabled]
  Queries value:
                                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ 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]
  Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
  Queries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
  Oueries value:
HKLM (system) current control set (services) winsock 2 parameters (names pace\_catalog\_catalog\_entries) (1) and (1) are the control set (1) are the c
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
  Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
  Queries value:
                                         HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Oueries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
                                          HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\feedplat[cachepath]
  Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
HKLM (system) current control set (services) winsock 2 parameters (namespace\_catalog S (catalog\_entries) (000000000002 [address family]) and the system (system) (s
  Oueries value
HKLM \\ system \\ current control set \\ services \\ winsock \\ parameters \\ name space \\ catalog \\ supported \\ name space \\ large \\ supported \\ name space \\ na
  Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ catalog\_entries \ 000000000002 \ [enabled]
  Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ catalog\_entries \ 000000000002 \ [version]
  Queries value:
Queries value:
Queries value:
Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
  Oueries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
                                          HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings \verb|\|5.0\> cache \verb|\| extensible | cache \verb|\| iecompat[cacherepair]|
  Oueries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
  Queries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
  Oueries value:
                                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
  Queries value:
                                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[providerid]
  Queries value:
Queries value:
Queries value:
Queries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]

```
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003[storesserviceclassinfo]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache
                                   nsible cache\ietld[cacheprefix]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\ietld[cachelimit]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings \verb|\|5.0| cache \verb|\|extensible| cache \verb|\|mshist012014033120140407[cacherepair]| \\
  Oueries value:
Queries value:
HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:
                                    HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
  Queries value:
                                    {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ tcpip \verb|\ parameters \verb|\ winsock[mapping]|
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [max sock addrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\e
                              ctensible cache\mshist012014041220140413[cachepath]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
  Queries value:
                                    \label{thm:local_equation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt local_equation} \mbox{\tt local_equation} \mbox{\tt local_equation} \mbox{\tt local_equation}} \mbox{\tt local_equation} \mbox{\tt local_
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cacherepair]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachepath]
                                    \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Queries value:
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
  Queries value:
                                    HKCU\software\microsoft\windows\cur
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[disableworkerthreadhibernation]
  Queries value
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings[socketsendbufferlength]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
  Queries value:
                                    \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[maxhttpredirects]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Oueries value:
                                    HKLM \verb|\software\microsoft\windows\currentversion\currenter|
settings[maxconnectionsperserver]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
{\tt settings[maxconnectionsper1\_0server]}
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Oueries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
                                    HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings[connectretries]
  Queries value:
                                    \label{lem:hklm} \verb+Kklm\+ software\+ incresoft\+ windows\+ current version\+ internet
settings[connectretries]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:
                                    HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:
                                    HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:
                                    \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{$\mbox{microsoft} \windows \current version} \end{tabular} \label{thm:local_hammon_hammon}
```

settings[disablentlmpreauth]

```
Oueries value
                          HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
                  henovalidate]
settings[certca
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings\5.0\cac
                          ngecachefilelimit]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[ftpdefaultexpir
                          ytimesecs]
 Oueries value:
                          HKLM\software\microsoft\internet
\verb|explorer\main\featurecontrol\feature_disable\_unicode\_handle\_closing\_callback[explorer.exe]| \\
 Queries value
                           HKLM\software\microsoft\internet
explorer\main\featur
                     econtrol\feature_disable_unicode_handle_closing_callback[*]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[leashlegacycookies]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablent4rasch
                          eck]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypassftpti
                      mecheck]
                          \label{thm:local_thm:local_thm} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet}} \\
 Queries value:
settings[releasesocketduringauth]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[releasesocketduring401auth]
 Queries value:
                           HKLM\softwar
                                         \microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
 Queries value
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
                      ocachecheck]
settings[bypasshttp
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
                          echeck]
settings[bypasssslnocach
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[enablehttptrace]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodia
                          override]
 Queries value:
                          HKCU\softwar
                                        e\microsoft\windows\currentversion\internet
{\tt settings[dontusednsloadbalancing]}
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[shareco
                 edswithwinhttp]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
 Queries value:
                           HKCU\software
                                          microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscachetimeout]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonpost]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnor
                          ing]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadce
                      tsending1
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbac
                          cving]
 Queries value:
                          \label{thm:local_thm:local_thm} \mbox{HKCU\software\mbox{\sc microsoft\windows\currentversion\sc internet}} \\
settings[warnonpostredirect]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[alwaysdrainonredirect]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonhttpstohttpredirect]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
 Queries value
                           HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[urlencoding]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilenam
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
```

```
settings[badproxyexpirestime]
                                              HKLM\sam\sam\domains\account\users\000003eb[v]
   Queries value:
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
   Queries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
                                             HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\profilelist[allusersprofile]
   Queries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
                                             HKLM\software\microsoft\windows\currentversion[programfilesdir]
   Oueries value:
                                              HKLM\software\microsoft\windows\currentversion[commonfilesdir]
   Oueries value:
   Queries value:
                                             \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} profile list \end{tabular} is the current version \end{tabular} and \end{tabular} in the current version \end{tabular} and \end{tabular} and \end{tabular} in the current version \end{tabular} and \end
1757981266-507921405-1957994488-1003[profileimagepath]
                                             HKCU\software\microsoft\windows
   Oueries value:
nt\currentversion\winlogon[parseautoexec]
   Queries value:
                                             HKLM\software\microsoft\internet
explorer \verb|\main| featurecontrol| feature_protocol_lockdown[reader\_sl.exe]|
   Queries value:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[winlogon.exe]
HKLM \verb|\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]|
   Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
   Oueries value:
                                              HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
   Queries value:
                                              HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
   Queries value:
                                              HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasapi32 [enable consolet racing]
   Oueries value:
                                              HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
                                              HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\rasapi32[filedirectory]
                                             \label{thm:local_hammon_hammon} HKLM \software \microsoft \tracing \netshell [filetracing mask] \\
   Queries value:
   Oueries value:
                                              HKLM\software\microsoft\tracing\netshell[enableconsoletracing]
   Queries value:
                                              \label{lem:hklm} \verb+Kklm| software| microsoft| tracing| netshell[consoletracingmask]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\netshell[maxfilesize]
   Oueries value:
                                              \label{lem:hklm} \verb+Kklm\+ software\+ icrosoft\+ tracing\+ netshell [filedirectory]
   Queries value:
                                              HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
   Queries value:
                                              HKLM\system\currentcontrolset\services\tapisrv\parameters[servicedll]
   Queries value:
                                              HKLM\system\currentcontrolset\services\tapisrv\parameters[servicemain]
                                              HKLM\software\microsoft\tracing\tapisrv[enabledebuggertracing]
   Queries value:
                                              HKLM\software\microsoft\tracing\tapisrv[enableconsoletracing]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\tapisrv[enablefiletracing]
                                             HKLM\software\microsoft\tracing\tapisrv[consoletracingmask]
HKLM\software\microsoft\tracing\tapisrv[filetracingmask]
   Queries value:
   Oueries value:
                                              HKLM\software\microsoft\tracing\tapisrv[maxfilesize]
   Queries value:
                                              HKLM\software\microsoft\tracing\tapisrv[filedirectory]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\wzctrace[enablefiletracing]
   Oueries value:
                                              \label{local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} wzctrace[filetracingmask] \\
                                              HKLM\software\microsoft\tracing\wzctrace[enableconsoletracing]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\wzctrace[consoletracingmask]
   Queries value:
                                              HKLM \setminus software \setminus microsoft \setminus tracing \setminus wzctrace[maxfilesize]
   Oueries value:
                                              HKLM\software\microsoft\tracing\wzctrace[filedirectory]
                                              HKLM\software\microsoft\tracing\eapol[enablefiletracing]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\eapol[filetracingmask]
   Queries value:
                                              HKLM\software\microsoft\tracing\eapol[enableconsoletracing]
   Queries value:
                                              HKLM\software\microsoft\tracing\eapol[consoletracingmask]
                                              {\tt HKLM \backslash software \backslash microsoft \backslash tracing \backslash eapol[maxfilesize]}
   Oueries value:
                                              HKLM\software\microsoft\tracing\eapol[filedirectory]
   Queries value:
                                              HKLM\software\microsoft\tracing\eapolqec[enablefiletracing]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\eapolqec[filetracingmask]
                                             HKLM\software\microsoft\tracing\eapolqec[enableconsoletracing]
HKLM\software\microsoft\tracing\eapolqec[consoletracingmask]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\eapolqec[maxfilesize]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\eapolqec[filedirectory]
                                             HKLM\software\microsoft\tracing\eapolqeccb[enablefiletracing]
HKLM\software\microsoft\tracing\eapolqeccb[filetracingmask]
   Oueries value:
   Oueries value:
                                              HKLM\software\microsoft\tracing\eapolqecb[enableconsoletracing]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\eapolqeccb[consoletracingmask]
   Queries value:
                                             HKLM\software\microsoft\tracing\eapolqeccb[maxfilesize]
HKLM\software\microsoft\tracing\eapolqeccb[filedirectory]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\svchost_rastls[enablefiletracing]
                                              HKLM\software\microsoft\tracing\svchost_rastls[filetracingmask]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\svchost_rastls[enableconsoletracing]
                                             HKLM\software\microsoft\tracing\svchost_rastls[consoletracingmask] HKLM\software\microsoft\tracing\svchost_rastls[maxfilesize]
   Oueries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\svchost_rastls[filedirectory]
   Oueries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\svchost_raschap[enablefiletracing]
   Queries value:
                                              HKLM \setminus software \setminus microsoft \setminus tracing \setminus svchost\_raschap[filetracing mask]
                                              HKLM\software\microsoft\tracing\svchost_raschap[enableconsoletracing]
   Oueries value:
                                              HKLM\software\microsoft\tracing\svchost_raschap[consoletracingmask]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\svchost_raschap[maxfilesize]
   Oueries value:
                                             HKLM\software\microsoft\tracing\svchost_raschap[filedirectory]
HKLM\software\microsoft\tracing\oneexsup[enablefiletracing]
   Oueries value:
                                              HKLM\software\microsoft\tracing\oneexsup[filetracingmask]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\oneexsup[enableconsoletracing]
   Queries value:
                                              HKLM \setminus software \setminus microsoft \setminus tracing \setminus one exsup[consoletracing mask]
                                             HKLM\software\microsoft\tracing\oneexsup[maxfilesize]
HKLM\software\microsoft\tracing\oneexsup[filedirectory]
   Oueries value:
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\wlpolicy[enablefiletracing]
   Queries value:
                                              HKLM\software\microsoft\tracing\wlpolicy[filetracingmask]
   Queries value:
                                              HKLM\software\microsoft\tracing\wlpolicy[enableconsoletracing]
                                              HKLM\software\microsoft\tracing\wlpolicy[consoletracingmask]
   Queries value:
                                              HKLM\software\microsoft\tracing\wlpolicy[maxfilesize]
   Queries value:
                                              HKLM\software\microsoft\tracing\wlpolicy[filedirectory]
   Queries value:
                                             \label{thm:hklm-soft-wave-microsoft-tracing-inpath-path-path-ing-inpath-path-ing-inpath-path-ing-inpath-path-inpath-path-inpath-path-inpath-path-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-inpath-in
   Queries value:
   Oueries value:
   Queries value:
                                              HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:
                                              HKLM\software\microsoft\com3[regdbversion]
   Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
```

settings[migrateproxy]

```
Oueries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
   Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
   Queries value:
                                              HKLM\software\microsoft\tracing\ipnathlp[enableconsoletracing]
   Queries value:
                                              HKLM\software\microsoft\tracing\ipnathlp[consoletracingmask]
   Oueries value:
                                              HKLM\software\microsoft\tracing\ipnathlp[maxfilesize]
   Queries value:
                                              HKLM \setminus software \setminus microsoft \setminus tracing \setminus ipnathlp[filedirectory]
                                              HKLM\software\microsoft\tracing\dot3api[enablefiletracing]
   Oueries value:
                                              HKLM\software\microsoft\tracing\dot3api[filetracingmask]
   Oueries value:
                                              HKLM \setminus software \setminus microsoft \setminus tracing \setminus dot 3 api[enable consoletracing]
   Queries value:
   Oueries value:
                                              HKLM \setminus software \setminus microsoft \setminus tracing \setminus dot 3 api[consoletracing mask]
                                             \label{lem:hklmsoftware} HKLM \software \mbox{\sc microsoft} tracing \dot3api \mbox{\sc maxfilesize}] \\ HKCR \clsid \dot465978620-5b9f-11d1-8dd2-
   Oueries value:
   Queries value:
00aa004abd5e}\inprocserver32[inprocserver32]
   Queries value:
                                             Queries value:
                                              HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\connections[defaultconnectionsettings]
                                              HKLM\software\microsoft\tracing\dot3api[filedirectory]
   Oueries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\netman[enablefiletracing]
                                             HKLM\software\microsoft\tracing\netman[filetracingmask]
HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}[appid]
   Queries value:
   Oueries value:
                                              HKCR\appid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}[dllsurrogate]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\netman[enableconsoletracing]
                                             \label{thm:consoft} HKLM \software \mbox{$^{\times}$ in the maniform of the manifold of the manif
   Oueries value:
   Oueries value:
                                              HKLM\software\microsoft\tracing\netman[filedirectory]
   Queries value:
                                              HKLM\software\microsoft\tracing\rasdlg[enablefiletracing]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\rasdlg[filetracingmask]
                                             \label{lem:hklmsoftware} HKLM \software \mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\m
   Oueries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\rasdlg[maxfilesize]
   Queries value:
   Queries value:
                                              HKLM\software\microsoft\tracing\rasdlg[filedirectory]
   Queries value:
                                             HKLM\system\currentcontrolset\control\productoptions[producttype]
   Queries value:
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus telephony [tapisrvwaithint]
   Queries value:
                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[explorer.exe]
                                             HKLM\software\microsoft\windows\currentversion\telephonv[min]
   Oueries value:
   Queries value:
                                              HKLM\software\microsoft\windows\currentversion\telephony[tapiscpttl]
                                              HKLM\software\microsoft\windows\currentversion\telephony[max]
   Queries value:
   Queries value:
                                             HKLM\software\microsoft\windows\currentversion\telephony[rpctimeout]
   Oueries value:
                                             HKLM\software\microsoft\windows\currentversion\telephony[domainname]
                                             HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
   Oueries value:
   Queries value:
                                             HKCR\clsid\{d5978620-5b9f-11d1-8dd2-
00aa004abd5e}\inprocserver32[threadingmodel]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapisrvnumhandlebuckets]
   Queries value:
                                             HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
   Queries value:
HKLM \verb|\system| current controlset \verb|\services| tapis rv \verb|\parameters[serviced]| lunload on stop] \\
                                             HKLM\svstem\currentcontrolset\services\rasman\parameters[servicedll]
   Oueries value:
   Queries value:
                                             HKLM\system\currentcontrolset\services\rasman\parameters[servicemain]
   Queries value:
Queries value:
                                             HKLM\system\currentcontrolset\services\rasman\parameters[prohibitipsec]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters[ipoutlowwatermark]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters[ipouthighwatermark]
Queries value: HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}[appid]
   Queries value:
                                             HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
   Queries value:
                                             HKCR\clsid\{5b035261-40f9-11d1-aaec-
00805fc1270e}\inprocserver32[inprocserver32]
   Queries value:
                                             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[dllsurrogate]
                                              HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[localservice]
   Queries value:
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
  Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
   Queries value:
                                             HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32[]
   Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[quervadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
   Queries value:
                                             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[]
   Queries value:
                                              HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[serviceparameters]
   Queries value:
                                             HKCR \ appid \ \{1be1f766-5536-11d1-b726-00c04fb926af\} [runas]
                                             \label{local-equation-of-control-equation} HKCR \ appid \ \{1be1f766-5536-11d1-b726-00c04fb926af\} [activateatstorage]
   Oueries value:
   Queries value:
HKLM \verb|\system| current control set \verb|\services| tcpip \verb|\parameters[used omain name devolution]| \\
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
   Queries value
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
HKLM \verb|\system| current controlset \verb|\services| dnscache \verb|\parameters[append to multilabel name]|
   Queries value:
```

```
HKLM\svstem\currentcontrolset\services\dnscache\parameters[screenbadtlds]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
     Queries value:
HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}[appid]
     Oueries value:
                                                                             HKLM\system\currentcontrolset\control\network[config]
     Queries value:
                                                                             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
      Queries value
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}[description]
                                                                             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[launchpermission]
     Queries value:
                                                                             HKLM\software\microsoft\ole[legacyauthenticationlevel]
     Oueries value:
      Oueries value:
                                                                             HKLM\software\microsoft\ole[legacyimpersonationlevel]
      Queries value:
                                                                             \label{local-equation} HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af\}[authenticationlevel]}
     Oueries value:
                                                                             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[remoteservername]
                                                                             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[srptrustlevel]
     Oueries value:
      Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
     Queries value:
                                                                             HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [useedns]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
     Queries value:
                                                                            HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [use hosts file]
     Oueries value:
HKLM\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]
     Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
     Queries value:
HKLM \verb|\system| current control set \verb|\services| train| and the substitution of the 
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
                                                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[svchost.exe]
                                                                             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
     Oueries value:
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[clsid]
                                                                             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
     Queries value:
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[service]
Queries \ value: \ HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\forall $$\arrowvert = 489e-84f0-d92eb38c0674\ndi[coservices]$
     Oueries value:
                                                                             08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[bindform]
     Queries value:
                                                                             08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[helptext]
    Queries value:
HKU\.default\software\microsoft\windows\shellnoroam\muicache[@netcfgx.dll,-50001]
     Queries value:
Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} set \color= \color=
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
     Queries value:
\label{local-parameters} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ is simplified by the control of the 
     Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
     Queries value:
Queries value:
\label{thm:local-control} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ is the local discount of the local disco
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
     Queries value:
                                                                             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318}\ford3b707-8bc4-489e-84f0-d92eb38c0674\}\ndi\interfaces[lowerexclude]
    Queries value:
                                                                             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318 \} \\ \{b7d3b707-8bc4-489e-84f0-d92eb38c0674\} \\ \\ \ndi\nterfaces[upperrange]
     Queries value:
                                                                             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi\interfaces[filtermediatypes]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
                                                                             HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
     Queries value:
      Queries value:
                                                                             HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
     Oueries value:
                                                                             HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
      Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
     Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
     Queries value
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
    Oueries value:
\label{thm:local_transform} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} evices \cite{topip} a rameters \cite{to
      Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} evices \cite{topip} arameters \c
     Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseobtainedtime]
c7d49d7cecdc}[leaseterminatestime]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
  Oueries value:
                               HKCR\clsid\{a907657f-6fdf-11d0-8efb-
00c04fd912b2}\inprocserver32[inprocserver32]
  Queries value:
                               HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Queries value:
                               HKCR\clsid\{1108be51-f58a-4cda-bb99
7a0227d11d5e}\inprocserver32[inprocserver32]
Oueries value: HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprocserver32[]
                               HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}[appid]
  Queries value:
                               \label{local-equation-of-hkkcr-appid-local-equation} \begin{tabular}{ll} HKCR \appid \ \{1be1f766-5536-11d1-b726-00c04fb926af\}[debugsurrogate] \end{tabular}
  Queries value:
                               HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprocserver32[]
HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}[appid]
  Oueries value:
  Oueries value:
                               HKLM\system\currentcontrolset\services\eventlog\system[primarymodule]
  Queries value:
  Oueries value:
                               HKLM\system\currentcontrolset\services\eventlog\system[eventmessagefile]
                               HKLM\system\currentcontrolset\services\eventlog\system\service control
  Queries value:
manager[categorymessagefile]
                               HKLM\svstem\currentcontrolset\services\eventlog\svstem\service control
  Oueries value:
manager[parametermessagefile]
  Queries value:
                               HKLM\system\currentcontrolset\services\eventlog\system\service control
manager[eventmessagefile]
                               HKCR\clsid\{a907657f-6fdf-11d0-8efb-
  Queries value:
00c04fd912b2}\inprocserver32[threadingmodel]
  Queries value:
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001[description]
  Oueries value
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi[clsid]
  Queries value
                               08002be10318}\0001\ndi[service]
  Queries value:
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi[coservices]
  Queries value:
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi[bindform]
  Queries value:
                               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[wmiprvse.exe]
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value:
08002be10318}\0001\ndi[helptext]
                               Queries value
08002be10318}\0001\ndi\interfaces[lowerrange]
Queries value: HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi\interfaces[lowerexclude]
                               Queries value:
08002be10318\} \verb|\| 0001\| interfaces[upperrange]
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value:
08002be10318}\0001\ndi\interfaces[filtermediatypes]
  Queries value:
c7d49d7cecdc}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[disableadapterdomainname]
  Queries value:
\label{thm:local_hkklm} \begin{tabular}{ll} HKLM \begin{tabular}{ll} 
c7d49d7cecdc}[registrationenabled]
  Queries value:
c7d49d7cecdc}[registeradaptername]
  Queries value:
c7d49d7cecdc}[registrationmaxaddresscount]
  Queries value:
c7d49d7cecdc}[maxnumberofaddressestoregister]
  Queries value:
c7d49d7cecdc}[domain]
  Oueries value
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008[description]
  Queries value:
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi[clsid]
  Queries value:
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi[service]
  Oueries value:
                               08002be10318}\0008\ndi[coservices]
  Queries value:
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi[bindform]
  Queries value
                               08002be10318}\0008\ndi[helptext]
  Queries value:
c7d49d7cecdc}[dhcpdomain]
  Queries value:
                               HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
00c04fb926af}\inprocserver32[inprocserver32]
  Queries value:
                               HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\nprocserver32[]
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value:
08002be10318}\0008\ndi\interfaces[lowerrange]
  Oueries value:
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi\interfaces[lowerexclude]
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi\interfaces[upperrange]
  Queries value:
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
```

```
08002be10318}\0008\ndi\interfaces[filtermediatypes]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[ipautoconfigurationenabled]
   Queries value:
c7d49d7cecdc}[addresstype]
c7d49d7cecdc}[nameserver]
   Oueries value:
c7d49d7cecdc}[dhcpnameserver]
   Queries value:
                                                 HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}[appid]
    Oueries value:
                                                 HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
                                                 HKLM\system\currentcontrolset\services\tcpip\parameters[nameserver]
    Queries value:
    Queries value:
                                                 HKLM\system\currentcontrolset\services\tcpip\parameters[ipenablerouter]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableicmpredirect]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[deadgwdetectdefault]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dontadddefaultgatewaydefault]
                                                HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
   Queries value:
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
                                                HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
                                                HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
   Oueries value:
00805fc79216\} \\ \text{ eventclasses } \\ \text{ } \\
00805fc79216\} \\ \text{ eventclasses } \\ \text{ } \\
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
   Queries value:
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
   Queries value:
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Oueries value:
                                                HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablesecurityfilters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\adapters\ndiswanip[ipinterfaces]
   Queries value:
\label{local-equation} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$
c7d49d7cecdc}[ipaddress]
   Oueries value:
c7d49d7cecdc}[subnetmask]
   Queries value:
HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[]
                                                  HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[version]
    Queries value:
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[defaultgateway]
   Oueries value:
c7d49d7cecdc}[defaultgatewaymetric]
   Oueries value:
                                                 HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0\win32[]
   Queries value:
c7d49d7cecdc}[interfacemetric]
   Oueries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[tcpallowedports]
  Queries value:
c7d49d7cecdc}[udpallowedports]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[rawipallowedprotocols]
  Oueries value:
c7d49d7cecdc}[activeconfigurations]
Queries value: HKCR\interface\{d597bab1-5b9f-11d1-8dd2-
00aa004abd5e}[interfacehelperdisabletypelib]
  Oueries value:
                               HKCR \verb| interface \verb| {d597bab1-5b9f-11d1-8dd2-1}|
00aa004abd5e}[interfacehelperdisableall1
  Queries value:
                               HKCR\interface\{d597bab1-5b9f-11d1-8dd2-
00aa004abd5e}[interfacehelperuser]
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
  Queries value:
00805fc79216}\subscriptions\{d789ab02-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
Queries value:
                               08002be10318\} \setminus \{61eab4e1-adba-45df-86af-11c0d7f92321\} \ [description]
                               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
  Queries value:
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[clsid]
                               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
  Queries value:
08002be10318 \} \\ \{ 61eab4e1-adba-45df-86af-11c0d7f92321 \} \\ \\ \  ndi[service]
                               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
  Oueries value:
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[coservices]
                               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
  Queries value:
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[bindform]
Queries \ value: \ HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-08002be10318\}\{61eab4e1-adba-45df-86af-11c0d7f92321\}\ndi[helptext]
  Queries value:
                               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
Oueries value:
                               08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces[lowerexclude]
  Queries value:
Queries value:
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces[upperrange]
Queries value: HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
Queries value:
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
  Queries value:
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
  Oueries value:
00805fc79216 \} subscriptions \{ f98c5003 - 16f4 - 4e33 - bca4 - e92f4742ad27 \} - \{ 00000000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 00000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000
Oueries value:
                               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
                               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216 \} subscriptions \{ f98c5003 - 16f4 - 4e33 - bca4 - e92f4742 ad27 \} - \{ 00000000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 00000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 000
Queries value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{16325b0b-4636-4303-
abe3-c7d49d7cecdc}[nameserverlist]
  Queries value:
abe3-c7d49d7cecdc}[netbiosoptions]
  Oueries value:
                               HKLM\system\currentcontrolset\services\rasman\parameters[medias]
  Queries value:
                               HKLM\software\microsoft\tracing\rastapi[enablefiletracing]
  Queries value:
                               {\tt HKLM \setminus software \setminus microsoft \setminus tracing \setminus rastapi[file tracing mask]}
                               HKLM\software\microsoft\eventsvstem\{26c409cc-ae86-11d1-b616-
  Oueries value:
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
Queries value:
                               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
                               HKLM\software\microsoft\tracing\rastapi[enableconsoletracing]
  Queries value:
                               HKLM\software\microsoft\tracing\rastapi[consoletracingmask]
  Queries value:
                               HKLM\software\microsoft\tracing\rastapi[maxfilesize]
                               HKLM\software\microsoft\tracing\rastapi[filedirectory]
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
  Queries value:
  Queries value:
00805fc79216}\subscriptions\{1ec466dd-2b44-4231-a775-cbd69f6eb46b}-{00000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
```

```
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Oueries value:
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
00805fc79216}\subscriptions\{4d99c768-0774-4b40-ac15-8342c658aad1}-{00000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
00805fc79216}\subscriptions\{68b25be9-46e1-45c1-8062-41b3d17a79a0}-{00000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{68b25be9-46e1-45c1-8062-41b3d17a79a0}-{00000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
00805fc79216}\subscriptions\{7f7b0a42-f639-4f28-9cf7-9338fedc54f0}-{00000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Oueries value:
00805fc79216}\subscriptions\{7f7b0a42-f639-4f28-9cf7-9338fedc54f0}-{00000000-0000-0000-0000-
Oueries value:
          HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Oueries value:
00805fc79216}\subscriptions\{913b976b-c04f-4957-90ef-c1ee4d66edfc}-{00000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\tracing\tapi32[enabledebuggertracing]
Queries value:
          HKLM\software\microsoft\tracing\tapi32[enableconsoletracing]
Oueries value:
Queries value:
          HKLM\software\microsoft\tracing\tapi32[enablefiletracing]
          HKLM\software\microsoft\tracing\tapi32[consoletracingmask]
HKLM\software\microsoft\tracing\tapi32[filetracingmask]
Queries value:
Oueries value:
          HKLM\software\microsoft\tracing\tapi32[maxfilesize]
Queries value:
          HKLM\software\microsoft\tracing\tapi32[filedirectory]
Queries value:
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
         HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{b8808a2b-4188-47e6-85ae-d3e76088cdae}-{00000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
```

```
Oueries value:
                                                                   HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
    Oueries value:
Oueries value:
                                                                   HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Oueries value:
                                                                   HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{0000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
    Queries value:
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
    Oueries value:
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
Queries value:
                                                                  HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
    Queries value:
HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
    Oueries value:
00805fc79216\} \setminus \{f98c5003 - 16f4 - 4e33 - bca4 - e92f4742ad27\} - \{00000000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 00000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 -
00805fc79216\} \setminus \{f98c5003 - 16f4 - 4e33 - bca4 - e92f4742ad27\} - \{00000000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 00000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 - 0000 -
Queries value:
HKU\. default\software\mbox{\mbox{$^$microsoft\windows\currentversion\telephony\handoffpriorities[request makecall]}}
    Oueries value:
HKU \verb|\| . default \verb|\| software \verb|\| microsoft \verb|\| windows \verb|\| current version \verb|\| telephony \verb|\| hand off priorities [request mediacall] | the first telephony \verb|\| current version \verb|\| telephony \verb|\| teleph
    Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[numproviders]
    Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid0]
    Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename0]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid1]
HKLM \verb|\software\microsoft\windows\currentversion\telephony\providers[providerfilename1]|
                                                                   HKLM\software\microsoft\tracing\kmddsp[enablefiletracing]
HKLM\software\microsoft\tracing\kmddsp[filetracingmask]
    Queries value:
     Queries value:
                                                                   HKLM\software\microsoft\tracing\kmddsp[enableconsoletracing]
     Queries value:
                                                                   HKLM\software\microsoft\tracing\kmddsp[consoletracingmask]
     Queries value:
    Oueries value:
                                                                   HKLM \setminus software \setminus microsoft \setminus tracing \setminus kmddsp[maxfilesize]
                                                                   HKLM\software\microsoft\tracing\kmddsp[filedirectory]
     Queries value:
    Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid2]
    Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename2]
    Queries value:
                                                                   HKLM\software\microsoft\tracing\ndptsp[enablefiletracing]
                                                                    HKLM\software\microsoft\tracing\ndptsp[filetracingmask]
     Queries value:
    Queries value:
                                                                   HKLM\software\microsoft\tracing\ndptsp[enableconsoletracing]
                                                                   HKLM \setminus software \setminus microsoft \setminus tracing \setminus ndptsp[consoletracingmask]
    Oueries value:
                                                                   HKLM\software\microsoft\tracing\ndptsp[maxfilesize]
    Queries value:
     Oueries value:
                                                                   HKLM\software\microsoft\tracing\ndptsp[filedirectory]
     Queries value:
HKLM \ software \ microsoft \ windows \ current version \ telephony \ providers [providerid3]
    Oueries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename3]
                                                                    HKLM\software\microsoft\tracing\conftsp[enabledebuggertracing]
    Queries value:
     Oueries value:
                                                                   HKLM \label{lem:hklm} In the latest and the lates
    Oueries value:
                                                                    HKLM\software\microsoft\tracing\conftsp[filetracingmask]
     Queries value:
     Queries value:
                                                                    HKLM\software\microsoft\tracing\conftsp[enableconsoletracing]
    Queries value:
                                                                   HKLM\software\microsoft\tracing\conftsp[maxfilesize]
     Oueries value:
                                                                   HKLM\software\microsoft\tracing\conftsp[filedirectory]
     Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\telephony\providers[providerid4]|
    Queries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} If the lemma \label{lem:hklm} is a simple constraint of the lemma \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hkklm} \label{lem
                                                                   HKLM\software\microsoft\windows\currentversion\h323tsp[debuglevel]
    Queries value:
     Oueries value
                                                                    HKLM\software\microsoft\windows\currentversion\h323tsp[q931listenport]
HKLM\software\microsoft\windows\currentversion\h323tsp[q931alertingtimeout]
    Oueries value:
HKLM \verb|\software\microsoft\windows\currentversion\h323tsp[h323gatewayaddress]|
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:hammon} \begin{tabular}{ll} HKLM 
                                                                   HKLM\software\microsoft\windows\currentversion\h323tsp[h323proxyaddress]
    Queries value:
```

```
Oueries value:
                               HKLM\software\microsoft\windows\currentversion\h323tsp[h323proxyenabled]
  Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in the constraint of the constrain
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gklogonphonenumberenabled]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gklogonaccountnameenabled]
  Queries value
Queries value:
HKLM\software\microsoft\windows\currentversion\telephonv\providers[providerfilename5]
  Oueries value
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000[netcfginstanceid]
  Oueries value
                              08002be10318}\0001[netcfginstanceid]
  Queries value
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002[netcfginstanceid]
  Queries value
                               08002be10318\} \verb|\\0003[netcfginstanceid]|
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value:
08002be10318}\0004[netcfginstanceid]
                              HKLM\system\o
  Queries value
                                               urrentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[netcfginstanceid]
  Queries value:
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[netcfginstanceid]
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value
08002be10318}\0006[wanendpoints]
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Oueries value:
08002be10318}\0006[enableforras]
  Queries value
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[enableforrouting]
 Queries value
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[enableforoutboundrouting]
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value
08002be10318}\0006[minwanendpoints]
  Oueries value
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[maxwanendpoints]
  Queries value
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[driverdesc]
  Queries value
                              08002be10318}\0006[fclientrole]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters[limitsimultaneousincomingcalls]
  Queries value:
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[calledidinformation]
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Queries value:
08002be10318}\0005[
                              dpoints]
  Queries value
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[enableforras]
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
 Oueries value
08002be10318}\0005[enableforrouting]
                              Queries value
08002 be 10318 \} \\ 0005 [enable for outbound routing]
 Queries value
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[minwanendpoints]
                              HKLM\system
  Queries value
                                               urrentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[maxwanendpoints]
 Oueries value
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[driverdesc]
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value
08002be10318}\0005[fclientrole]
 Queries value
                              08002be10318}\0005[calledidinformation]
  Queries value
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[wanendpoints]
  Oueries value
                              HKLM\sys1
                                           em\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[enableforras]
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value
08002be10318}\0004[enableforrouting]
  Queries value:
                              08002be10318}\0004[enableforoutboundrouting]
 Queries value:
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318\0004[minwanendpoints]
  Queries value
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[maxwanendpoints]
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value:
08002be10318}\0004[driverdesc]
  Queries value:
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[fclientrole]
 Oueries value
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[calledidinformation]
                               HKLM\system\curr
  Queries value
                                                  entcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[netcfginstanceid]
 Queries value
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[wanendpoints]
  Queries value
                               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[enableforras]
  Oueries value
                              08002be10318}\0007[enableforrouting]
  Queries value
                               08002be10318}\0007[enableforoutboundrouting]
  Queries value
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[minwanendpoints]
                              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
  Queries value:
08002be10318}\0007[maxwanendpoints]
  Queries value
                              08002be10318}\0007[driverdesc1
  Queries value:
                              08002be10318}\0007[fclientrole]
                              Queries value
```

08002be10318}\0007[calledidinformation]

```
Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters\quarantine[enabled]
                                            HKLM\software\microsoft\tracing\rasqec[enablefiletracing]
   Queries value:
   Oueries value:
                                            HKLM\software\microsoft\tracing\rasqec[filetracingmask]
                                           HKLM\software\microsoft\tracing\rasqec[enableconsoletracing]
   Oueries value:
                                            HKLM\software\microsoft\tracing\rasqec[consoletracingmask]
   Queries value:
   Queries value:
                                            HKLM\software\microsoft\tracing\rasqec[maxfilesize]
   Queries value:
                                            HKLM\software\microsoft\tracing\rasqec[filedirectory]
   Queries value:
                                            {\tt HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasman[enable file tracing]}
                                            HKLM\software\microsoft\tracing\rasman[filetracingmask]
   Oueries value:
                                            HKLM\software\microsoft\tracing\rasman[enableconsoletracing]
   Oueries value:
                                            Queries value:
   Oueries value:
                                           {\tt HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasman[maxfilesize]}
   Oueries value:
                                            HKLM\software\microsoft\tracing\rasman[filedirectory]
   Queries value:
HKLM\software\microsoft\tracing\ppp[enablefiletracing]
HKLM\software\microsoft\tracing\ppp[filetracingmask]
   Queries value:
   Queries value:
                                            HKLM\software\microsoft\tracing\ppp[enableconsoletracing]
   Queries value:
                                            HKLM\software\microsoft\tracing\ppp[consoletracingmask]
   Queries value:
   Oueries value:
                                            HKLM\software\microsoft\tracing\ppp[maxfilesize]
                                           HKLM\software\microsoft\tracing\ppp[filedirectory]
HKLM\software\microsoft\tracing\bap[enablefiletracing]
   Oueries value:
   Queries value:
   Oueries value:
                                            HKLM\software\microsoft\tracing\bap[filetracingmask]
                                            HKLM\software\microsoft\tracing\bap[enableconsoletracing]
   Queries value:
   Queries value:
                                            HKLM \setminus software \setminus microsoft \setminus tracing \setminus bap[consoletracing mask]
                                            HKLM\software\microsoft\tracing\bap[maxfilesize]
   Oueries value:
   Queries value:
                                            HKLM\software\microsoft\tracing\bap[filedirectory]
   Queries value:
                                            HKLM\system\currentcontrolset\services\rasman\ppp[maxterminate]
   Oueries value:
                                            HKLM \verb|\system| current control set \verb|\services| rasman \verb|\ppp[maxconfigure]|
                                            HKLM\svstem\currentcontrolset\services\rasman\ppp[maxfailure]
   Oueries value:
   Queries value:
                                            HKLM\system\currentcontrolset\services\rasman\ppp[maxreject]
                                            HKLM\system\currentcontrolset\services\rasman\ppp[restarttimer]
   Queries value:
   Queries value:
                                            HKLM\system\currentcontrolset\services\rasman\ppp[negotiatetime]
   Oueries value:
                                            {\tt HKLM \ } system \verb|\ current controlset \ | services \verb|\ rasman \ | ppp[default callback delay]|
                                            HKLM\system\currentcontrolset\services\rasman\ppp[defaultportlimit]
   Queries value:
   Queries value:
                                            HKLM\system\currentcontrolset\services\rasman\ppp[defaultsessiontimeout]
   Queries value:
                                            HKLM\system\currentcontrolset\services\rasman\ppp[defaultidletimeout]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp[lowerbandwidththreshold]
   Queries value:
                                            HKLM\system\currentcontrolset\services\rasman\ppp[timebelowtheshold]
   Queries value:
                                           HKLM\system\currentcontrolset\services\rasman\ppp[baplistentimeout]
   Oueries value:
HKLM\system\currentcontrolset\services\rasman\ppp[unknownpackettracesize]
   Queries value:
                                           HKLM\system\currentcontrolset\services\rasman\ppp[echorequestinterval]
   Queries value:
                                            HKLM\system\currentcontrolset\services\rasman\ppp[idletimebeforeecho]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp[missedechosbeforedisconnect]
  Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ is simple for the property of the property of
                                           HKLM\system\currentcontrolset\services\rasman\ppp[parsedllpath]
   Queries value:
   Oueries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[path]
   Queries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiatecbcp]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateccp]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateipx]
   Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiatepap]] \end{tabular}
   Queries value
Queries value:
\label{thm:local_system} HKLM \system \current controls et\services \rasman \ppp \control protocols \builtin[negotiatespap] \\
   Queries value:
\label{thm:loss} HKLM \software \mbox{$\mbox{$\mbox{$\rm HKLM}$} irrosoft \racing \rasspap [file tracing mask]} \\
   Oueries value:
   Queries value:
   Oueries value:
                                            HKLM\software\microsoft\tracing\rasspap[enableconsoletracing]
   Queries value:
                                            HKLM\software\microsoft\tracing\rasspap[consoletracingmask]
   Queries value:
                                           HKLM \backslash software \backslash microsoft \backslash tracing \backslash rasspap [maxfile size] \\
   Oueries value:
                                            HKLM\software\microsoft\tracing\rasspap[filedirectory]
   Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} N system \current control set \end{tabular} restricts equencing \end{tabular}
   Queries value:
                                           \label{thm:loss} HKLM \noindent \n
   Oueries value:
   Queries value:
                                            HKLM\software\microsoft\tracing\raspap[enableconsoletracing]
   Queries value:
                                            HKLM\software\microsoft\tracing\raspap[consoletracingmask]
   Queries value:
                                            HKLM\software\microsoft\tracing\raspap[maxfilesize]
                                           \label{thm:local-problem} HKLM \software \mbox{$\mbox{$\tt MKLM}$} in \software \mbox{$\tt microsoft} \mbox{$\mbox{$\tt tracing}$} raseap \soling \mbox{$\tt enable file tracing} \label{tracing}
   Oueries value:
   Queries value:
   Queries value:
                                            HKLM\software\microsoft\tracing\raseap[filetracingmask]
   Oueries value:
                                            HKLM\software\microsoft\tracing\raseap[enableconsoletracing]
   Queries value:
                                            HKLM \setminus software \setminus microsoft \setminus tracing \setminus raseap[consoletracing mask]
                                            HKLM\software\microsoft\tracing\raseap[maxfilesize]
   Queries value:
   Queries value:
                                            HKLM\software\microsoft\tracing\raseap[filedirectory]
                                            HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[path]
   Queries value:
                                           HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[path] HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[path]
   Queries value:
   Oueries value:
   Queries value:
                                            HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[path]
   Queries value:
                                            HKLM\software\microsoft\tracing\rasccp[enablefiletracing]
   Oueries value:
                                            HKLM\software\microsoft\tracing\rasccp[filetracingmask]
```

HKLM\software\microsoft\tracing\rasccp[enableconsoletracing]

HKLM\svstem\currentcontrolset\services\rasman\parameters[numberofrings]

Oueries value:

Oueries value:

```
{\tt HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasccp[consoletracing mask]}
     Oueries value:
                                                                              HKLM\software\microsoft\tracing\rasccp[maxfilesize]
     Queries value:
     Queries value:
                                                                              HKLM\software\microsoft\tracing\rasccp[filedirectory]
                                                                              HKLM\software\microsoft\tracing\rasbacp[enablefiletracing]
      Queries value:
     Queries value:
                                                                              HKLM\software\microsoft\tracing\rasbacp[filetracingmask]
                                                                              \label{localization} \begin{tabular}{ll} HKLM\software\mbox{\sc microsoft}\tracing\sc mash{\sc microsoft}\tracing\sl\c mash{\sc mi
     Oueries value:
                                                                              HKLM\software\microsoft\tracing\rasbacp[consoletracingmask]
     Queries value:
      Queries value:
                                                                              HKLM\software\microsoft\tracing\rasbacp[maxfilesize]
     Oueries value:
                                                                              HKLM\software\microsoft\tracing\rasbacp[filedirectory]
     Queries value:
                                                                              HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasiphlp[enablefile tracing]
                                                                              HKLM\software\microsoft\tracing\rasiphlp[filetracingmask]
     Oueries value:
                                                                              HKLM\software\microsoft\tracing\rasiphlp[enableconsoletracing]
      Oueries value:
     Queries value:
                                                                              HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasiphlp[consoletracing mask]
     Oueries value:
                                                                             HKLM \setminus software \setminus microsoft \setminus tracing \setminus rasiphlp[maxfilesize]
                                                                              HKLM\software\microsoft\tracing\rasiphlp[filedirectory]
     Oueries value:
                                                                              HKLM\software\microsoft\rpc\securityservice[10]
      Queries value:
      Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
     Queries value:
     Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
     Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
     Queries value:
                                                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
      Oueries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \cite{LM} & system \cite{LM} &
     Queries value:
                                                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
     Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
     Queries value:
                                                                              HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
      Queries value:
                                                                             HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus digest. dll[comment]
     Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
      Queries value:
                                                                             HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
     Queries value:
                                                                             HKLM \setminus system \setminus current control \setminus lsa \setminus spicache \setminus digest.dll[version]
     Oueries value:
                                                                             HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
     Queries value:
HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus digest.dll[tokensize]
     Queries value:
                                                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
     Queries value:
                                                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
     Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
     Queries value:
                                                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
      Oueries value:
                                                                             Oueries value:
                                                                             HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
     Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
     Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[usedhcpaddressing]
    Queries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} and $$ ip[network adapter guid] $$ in the local property of the local property of
     Queries value:
HKLM\svstem\currentcontrolset\services\remoteaccess\parameters\ip[suppresswinsnameservers]
     Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[suppressdnsnameservers]
     Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[initialaddresspoolsize]
    Oueries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[allownetworkaccess]
     Queries value:
Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[winsnameserverbackup]
\label{thm:local_thm} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} set \current control set \current co
     Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\adapters\ndiswanip[ipconfig]
    Queries value:
fb0d4cf73262}[dhcpipaddress]
    Queries value:
fb0d4cf73262}[dhcpsubnetmask]
     Queries value:
HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{4fe87b73-b12e-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-82c4-47d6-8
fb0d4cf73262}[domain]
      Oueries value:
fb0d4cf73262}[nameserver]
     Oueries value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{4fe87b73-b12e-47d6-properties}
82c4-fb0d4cf73262}[nameserverlist]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[dhcpipaddress]
     Queries value:
e3686652faee}[dhcpsubnetmask1
    Queries value:
e3686652faee}[domain]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[nameserver]
     Queries value:
HKLM \ system \ current control set \ \ net b t) parameters \ interfaces \ \ tcpip_{cac79791-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-bd6d-4f3e-b
bcad-e3686652faee}[nameserverlist]
     Queries value:
Oueries value:
                                                                             HKLM\software\microsoft\tracing\rasipcp[enablefiletracing]
```

HKLM\software\microsoft\tracing\rasipcp[filetracingmask]

Oueries value:

```
HKLM\software\microsoft\tracing\rasipcp[enableconsoletracing]
   Oueries value:
                                                  HKLM\software\microsoft\tracing\rasipcp[consoletracingmask]
   Queries value:
    Queries value:
                                                  HKLM\software\microsoft\tracing\rasipcp[maxfilesize]
                                                  HKLM\software\microsoft\tracing\rasipcp[filedirectory]
    Queries value:
   Queries value:
                                                  HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[spoolsv.exe]
   Queries value:
HKLM\system\currentcontrolset\control\networkprovider\hworder[providerorder]
   Queries value:
                                                  HKLM\system\currentcontrolset\services\rdpnp\networkprovider[name]
   Queries value:
                                                  HKLM\system\currentcontrolset\services\rdpnp\networkprovider[class]
   Oueries value:
HKLM\system\currentcontrolset\services\rdpnp\networkprovider[providerpath]
   Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[name]
   Oueries value:
\label{thm:local_hamman_hamman} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{tabular} $$ is simplified by the local control set \end{
   Queries value:
HKLM \verb|\system| current controlset \verb|\services| lanman work station \verb|\networkprovider| [provider path]|
                                                  HKLM\system\currentcontrolset\services\webclient\networkprovider[name]
   Queries value:
                                                  HKLM\system\currentcontrolset\services\webclient\networkprovider[class]
    Queries value:
    Queries value:
HKLM\system\currentcontrolset\services\webclient\networkprovider[providerpath]
                                                  HKLM\software\microsoft\windows nt\currentversion\network\world full
   Oueries value:
access shared parameters[sort hyphens]
    Oueries value:
                                                  HKLM\software\microsoft\wbem\cimom[logging]
                                                  HKLM\software\microsoft\wbem\cimom[log file max size]
    Queries value:
   Queries value:
                                                  HKCR\clsid\{4fa18276-912a-11d1-ad9b-
00c04fd8fdff}\inprocserver32[inprocserver32]
   Queries value:
                                                  HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\nprocserver32[]
    Queries value:
                                                  HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff\}[appid]
   Oueries value:
                                                  HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-
5e7582d8c9fa}\inprocserver32[inprocserver32]
                                                  HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprocserver32[]
   Queries value:
                                                  HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}[appid]
    Queries value:
   Queries value:
                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ perflib[disable]
performance counters1
                                                  HKLM\software\microsoft\internet
   Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[jqs.exe]
    Queries value:
                                                  HKLM\software\microsoft\wbem\cimom[working directory]
   Queries value:
                                                  HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
    Queries value:
                                                  HKCU\appevents\schemes\apps\.default\systemnotification\.current[]
    Queries value:
                                                  HKLM\software\microsoft\windows
nt\currentversion\compatibility32[wmiadap]
                                                  HKLM\software\microsoft\windows nt\currentversion\ime
   Oueries value:
compatibility[wmiadap]
    Queries value:
                                                  HKLM\software\microsoft\wbem\cimom[logging directory]
    Queries value:
                                                  HKLM\software\microsoft\wbem\cimom[repository directory]
   Oueries value:
                                                  HKU\.default\control panel\international[locale]
   Queries value:
                                                  HKLM\system\currentcontrolset\control\nls\locale[00000409]
    Queries value:
                                                  HKLM\system\currentcontrolset\control\nls\language groups[1]
    Queries value:
                                                  HKU\.default\control panel\international[scurrency]
   Oueries value:
                                                  HKU\.default\control panel\international[smondecimalsep]
                                                  {\tt HKU} \verb|.default| control panel| international[smonthousandsep]|\\
   Queries value:
    Queries value:
                                                  HKU\.default\control panel\international[smongrouping]
    Queries value:
                                                  HKU\.default\control panel\international[spositivesign]
   Queries value:
                                                  HKU\.default\control panel\international[snegativesign]
   Oueries value:
                                                  HKU\.default\control panel\international[icurrdigits]
                                                  HKU\.default\control panel\international[sdecimal]
   Queries value:
                                                   HKU\.default\control panel\international[sthousand]
    Queries value:
   Queries value:
                                                  HKU\.default\control panel\international[sgrouping]
   Queries value:
                                                  HKU \verb|\|.default\\| control panel\\| international[s1159]
                                                  HKU\.default\control panel\international[s2359]
   Queries value:
                                                  HKU\.default\control panel\international[sshortdate]
    Queries value:
    Queries value:
                                                  HKU\.default\control panel\international[slongdate]
   Oueries value:
                                                  HKU\.default\control panel\international[stimeformat]
                                                  HKU\.default\control panel\international[icalendartype]
   Oueries value:
                                                  HKLM\software\microsoft\rpc[maxrpcsize]
   Queries value:
                                                  \label{local-operator} \begin{tabular}{ll} HKLM \end{tabular} $$ KLM \end{tabular} in the interestion \end{tabular} in the interestion \end{tabular} $$ in the interestion \
    Queries value:
    Queries value:
                                                  HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 1]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
    Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
    Queries value:
   Queries value:
                                                  HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [wave 5]
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
   Queries value:
                                                   HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
    Oueries value:
    Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midil]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
    Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
   Oueries value:
                                                  HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 \\ [midi4]
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
   Oueries value:
    Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
    Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
   Queries value:
                                                  HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [midi8]
                                                  \label{thm:loss} $HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] $HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] $$
   Oueries value:
   Queries value:
    Queries value:
                                                  HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 1]
    Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
   Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
    Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
    Queries value:
   Queries value:
                                                  Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
    Queries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
    Queries value:
\label{thm:local_model} \begin{tabular}{ll} HKLM \end{tabular} $$ KLM \end{tabular} $$ HKLM \end{tabular} $$ is a control \e
   Oueries value:
                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
```

```
Oueries value:
                                                                                                          HKI M\software\microsoft\windows nt\currentyersion\drivers32[mixer1]
                                                                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
       Queries value:
       Queries value:
                                                                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
        Queries value:
                                                                                                          HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [mixer 4]
       Queries value:
                                                                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
                                                                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
       Oueries value:
                                                                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
       Queries value:
                                                                                                          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
        Queries value:
       Queries value:
                                                                                                         HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
       Queries value:
                                                                                                          HKU\.default\software\microsoft\multimedia\audio[systemformats]
                                                                                                         HKLM\software\microsoft\windows
       Oueries value:
nt\currentversion\drivers32[msacm.imaadpcm]
       Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
       Oueries value:
\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$ \end{tabular} $$ HKLM \end{tabular} $$ in a adpcm [cformattags] $$ \end{tabular} $$ \end{tabular} $$ in a adpcm [cformattags] $$ in a constant $$ in a constan
       Queries value
HKLM \verb|\software\microsoft| audiocompression manager \verb|\drivercache| microsoft| audiocompression microsoft| microso
      Queries value:
\label{local-prop} \mbox{HKLM} \mbox{$\  \  \  } \mbox{$\  $ \  \  $\  \  )$ in a adpcm [cfilter tags] $$
       Queries value:
                                                                                                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msadpcm]
       Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
       Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
       Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
       Queries value:
\label{thm:local_hammager} \label{thm:local_hammager} HKLM \label{thm:local_hammager} In the local content of th
       Queries value:
                                                                                                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg711]
       Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
       Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
      Queries value:
HKLM \verb|\software| microsoft| audio compression manager \verb|\driver| cache| msacm.msg711[afor mattag cache] is a constant of the constant of th
       Queries value:
HKLM \backslash software \backslash microsoft \backslash audio compression manager \backslash driver cache \backslash msacm. msg711[cfilter tags]
       Queries value:
                                                                                                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msgsm610]
       Queries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msgsm610 [fdwsupport]
      Oueries value:
Queries value:
\label{thm:local} HKLM \label{thm:local} \begin{tabular}{ll} HKLM \label{thm:local} software \end{tabular} in the local discontinuous constraints of the local discontinuous constraints and the local discontinuous constraints are also as a local discontinuous constraint. \\
       Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
       Queries value:
                                                                                                          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.trspch]
       Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
       Queries value:
HKLM \verb|\software\microsoft\audiocompression manager\driver cache \verb|\msacm.trspch| [cformattags]| \\
       Queries value:
HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm.trspch[aformattagcache]
       Queries value:
\label{thm:local_hamma} \begin{tabular}{ll} HKLM \end{tabular} $$ KLM \end{tabular} $$ HKLM \end{tabular} $$ Audio compression manager \end{tabular} $$ 
       Queries value:
                                                                                                         HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg723]
       Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
       Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
       Oueries value:
\label{thm:macmmag} \begin{tabular}{ll} HKLM \end{tabular} software \verb|\microsoft| audiocompression manager \end{tabular} driver cache \end{tabular} msg723 [a formattag cache] and the same microsoft \end{tabular} are the same manager \end{tabular} are the same
       Queries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msg723 [cfilter tags]
                                                                                                          HKLM\software\microsoft\windows
      Queries value:
nt\currentversion\drivers32[msacm.msaudio1]
       Queries value:
HKLM \label{lem:hklm} If the discontinuous of the discontinuous of the latest and the discontinuous of the latest and the la
      Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
        Oueries value:
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1\cfiltertags1
                                                                                                         HKLM\software\microsoft\windows
      Queries value:
nt\currentversion\drivers32[msacm.sl_anet]
       Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[fdwsupport]
       Queries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. sl\_anet[cformattags]
       Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
       Queries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. sl\_anet[cfilter tags]
                                                                                                         HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
       Queries value:
       Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
       Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
       Queries value:
HKLM \ \ software \ \ \ \ iac2[a formattag cache]
       Queries value:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.iac2[cfiltertags]
        Oueries value:
                                                                                                         \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} in the current version \end{tabular} are the curre
       Oueries value:
```

```
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.13acm[fdwsupport]
 \label{thm:local_hamma} \begin{tabular}{ll} HKLM \end{tabular} $$ KLM \end{tabular} $$ HKLM \end{tabular} $$ Audio compression manager \end{tabular} $$ 
    Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
    Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.13acm[cfiltertags]
                                                              HKU\.default\software\microsoft\multimedia\audio compression
    Queries value:
manager\msacm[nopcmconverter]
    Queries value:
                                                             HKU\.default\software\microsoft\multimedia\audio compression
manager\priority v4.00[prioritv1]
                                                             HKU\.default\control panel\desktop[smoothscroll]
    Queries value:
                                                             HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
                                                             HKLM\software\microsoft\windows
    Oueries value:
 nt\currentversion\winlogon[chkaccdebuglevel]
    Queries value:
                                                              HKU\.default\software\microsoft\windows\currentversion\explorer\user
 shell folders[personal]
                                                             HKU\.default\software\microsoft\windows\currentversion\explorer\user
    Queries value:
shell folders[local settings]
                                                             HKLM\software\microsoft\windows
    Queries value:
 nt\currentversion\winlogon[rsopdebuglevel]
                                                             HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
    Oueries value:
    Queries value:
HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| the memanager[compositing]| | the memanager and the memanager are compositing and the memanager are compositions and the memanager are compositions and the memanager are compositions are compositions and the memanager are compositions are compositions and the memanager are compositions are compositions are compositions and the memanager are compositions are compositions are compositions and the memanager are compositions are compositions are compositions are compositions and the memanager are compositions are compo
                                                              HKU\.default\control panel\desktop[lamebuttontext]
     Queries value:
    Queries value:
                                                             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature protocol lockdown[wmiadap.exe]
    Queries value:
                                                             HKLM\software\microsoft\ole[maximumallowedallocationsize]
     Queries value:
                                                              HKLM \setminus system \setminus current control \setminus lsa[everyone includes an onymous]
     Queries value:
                                                              {\tt HKLM \setminus software \setminus microsoft \setminus wbem \setminus cimom[adapperflib max size blob collect]}
                                                              HKLM\software\microsoft\wbem\cimom[processid]
    Queries value:
     Queries value:
                                                              HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
     Queries value:
                                                              HKLM\software\microsoft\com3[com+enabled]
    Queries value:
                                                              {\tt HKLM \setminus software \setminus microsoft \setminus ole[minimumfreemempercentage to create process]}
                                                             Oueries value:
    Queries value:
 00aa004b2e24}\inprocserver32[inprocserver32]
                                                             HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]
     Queries value:
     Queries value:
                                                              HKCR\clsid\{4590f811-1d3a-11d0-891f-
    Queries value:
 00aa004b2e24}\inprocserver32[threadingmodel]
     Queries value:
                                                              HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
     Oueries value:
                                                             HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[dllsurrogate]
HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
    Oueries value:
    Queries value:
                                                              HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
     Queries value:
                                                              HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[serviceparameters]
    Queries value:
                                                             \label{local-hkcr} $HKCR\appid_{8bc3f05e-d86b-11d0-a075-00c04fb68820}[runas]$ $HKCR\appid_{8bc3f05e-d86b-11d0-a075-00c04fb68820}[activate at storage]$ $HKCR^appid_{8bc3f05e-d86b-11d0-a075-00c04fb68820}[activate at stora
    Oueries value:
                                                              HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[launchpermission]
    Queries value:
                                                              HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[authenticationlevel]
     Queries value:
     Queries value:
                                                              HKCR \label{locality} LRCR \label{locality} HKCR \label{locality} ICR \label{locality} HKCR \label{locality} HKCR \label{locality} HKCR \label{locality} ICR \label{locality} HKCR \label{locality} ICR \label{locality} HKCR \label{locality} HKCR \label{locality} HKCR \label{locality} ICR \label{locality} HKCR \label{locality} HK
                                                              HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[srptrustlevel]
    Oueries value:
                                                              HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[debugsurrogate]
    Queries value:
    Queries value:
                                                             HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[inprocserver32]
    Queries value:
                                                             HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
                                                             HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
    Oueries value:
                                                              HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32[]
    Queries value:
                                                              HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
                                                             Queries value:
    Queries value:
ce99a996d9ea}\inprocserver32[inprocserver32]
    Queries value:
                                                             HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
                                                             HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
     Oueries value:
     Oueries value:
    Queries value:
                                                             HKCR\clsid\{d68af00a-29cb-43fa-8504-
 ce99a996d9ea}\inprocserver32[threadingmodel]
    Queries value:
                                                             {\tt HKLM \setminus software \setminus microsoft \setminus wbem \setminus cimom[enable private object heap]}
                                                             HKLM\software\microsoft\wbem\cimom[contextlimit]
    Queries value:
     Queries value:
                                                              HKLM\software\microsoft\wbem\cimom[objectlimit]
                                                              HKLM\software\microsoft\wbem\cimom[identifierlimit]
     Queries value:
    Queries value:
                                                             HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-
2a3b153b886d}\inprocserver32[inprocserver32]
                                                             HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}\inprocserver32[]
    Queries value:
                                                              HKCR\clsid\{cd1abfc8-6c5e-4a8d-b90b-2a3b153b886d}[appid]
     Queries value:
                                                             HKCR\clsid\{9a653086-174f-11d2-b5f9-
HKCR\clsid\{9a653086-174f-11d2-b5f9-00104b703efd}[appid]
     Queries value:
     Queries value:
                                                             HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
                                                             HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
    Queries value:
                                                              HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[appid]
     Queries value:
     Queries value:
                                                              HKCR\interface\{027947e1-d731-11ce-a357-00000000001}\proxystubclsid32[]
     Queries value:
                                                             HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32[]
                                                              HKCR\clsid\{cc9072ab-c000-49d8-a5aa-
00266c8dbb9b}\inprocserver32[inprocserver32]
    Queries value:
                                                             HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}\inprocserver32[]
                                                             HKCR\clsid\{cc9072ab-c000-49d8-a5aa-00266c8dbb9b}[appid]
     Queries value:
                                                             HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]
     Oueries value:
                                                             HKCR\clsid\{d2d588b5-d081-11d0-99e0-
     Queries value:
00c04fc2f8ec}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{d2d588b5-d081-11d0-99e0-
 00c04fc2f8ec}\inprocserver32[synchronization]
     Queries value:
                                                             HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}\inprocserver32[]
     Oueries value:
                                                             HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}[]
                                                             HKCR\clsid\{d2d588b5-d081-11d0-99e0-00c04fc2f8ec}[appid]
    Oueries value:
```

```
Oueries value:
                          HKCR\clsid\{eac8a024-21e2-4523-ad73-
a71a0aa2f56a}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{eac8a024-21e2-4523-ad73-a71a0aa2f56a}\inprocserver32[]
                           \label{locality} $$ HKCR\clsid{eac8a024-21e2-4523-ad73-a71a0aa2f56a}[appid] $$
  Queries value:
 Queries value
                           HKCR\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[inprocserver32]
                          HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\inprocserver32[]
 Queries value:
                           HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}[appid]
  Queries value:
 Queries value:
                          HKCR\clsid\{4590f812-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
                          HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
 Oueries value:
                           HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}[appid]
  Oueries value:
                          HKCR\clsid\{eac8a024-21e2-4523-ad73-
 Queries value:
a71a0aa2f56a}\inprocserver32[threadingmodel]
                          HKCR\clsid\{d2d588b5-d081-11d0-99e0-
 Oueries value:
00c04fc2f8ec}\inprocserver32[inprocserver32]
 Queries value
                          HKLM\system\currentcontrolset\control\wmi\security[b48d49a2-e777-11d0-
a50c-00a0c90629101
                          HKLM\system\currentcontrolset\control\wmi\security[b48d49a3-e777-11d0-
 Queries value:
a50c-00a0c9062910]
 Queries value:
                           HKLM\system\currentcontrolset\control\wmi\security[05901221-d566-11d1-
b2f0-00a0c90629101
 Oueries value:
                           HKLM\svstem\currentcontrolset\services\acpi[mofimagepath]
 Queries value:
                           HKLM\system\currentcontrolset\services\acpi[imagepath]
  Oueries value:
                           HKLM\system\currentcontrolset\services\mssmbios[mofimagepath]
                           HKLM\system\currentcontrolset\services\mssmbios[imagepath]
  Queries value:
 Queries value:
                           HKLM\system\currentcontrolset\services\pcnet[mofimagepath]
                           HKLM\svstem\currentcontrolset\services\pcnetfimagepathl
 Oueries value:
 Queries value:
                           HKLM\system\currentcontrolset\services\ipnat[mofimagepath]
  Queries value:
                           HKLM\system\currentcontrolset\services\ipnat[imagepath]
  Queries value:
                           {\tt HKLM \ } system \verb| current control set \verb| services \verb| http[mofimage path]|
 Oueries value:
                           HKLM\system\currentcontrolset\services\http[imagepath]
                           HKCR\clsid\{c10b4771-4da0-11d2-a2f5-
 Queries value:
00c04f86fb7d}\inprocser
                         ver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}\\\\\\\\\\\\
                          HKCR\clsid\{c10b4771-4da0-11d2-a2f5-00c04f86fb7d}[appid]
  Oueries value:
                          HKCR\clsid\{c10b4771-4da0-11d2-a2f5-
 Queries value:
00c04f86fb7d}\inprocserver32[threadingmodel]
  Queries value:
                          {\tt HKLM \setminus software \setminus microsoft \setminus wbem \setminus cimom[enable private mof dheap]}
 Queries value:
                          HKCR\clsid\{cb8555cc-9128-11d1-ad9b-
00c04fd8fdff}\inprocserver32[inprocserver32]
  Queries value:
                          HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff}\inprocserver32[]
  Queries value:
                           HKCR\clsid\{cb8555cc-9128-11d1-ad9b-00c04fd8fdff\}[appid]
 Oueries value:
                          HKCR \verb|\clsid| \{ cb8555cc-9128-11d1-ad9b-
00c04fd8fdff}\inprocserver32[threadingmodel]
                          HKLM\software\microsoft\internet
 Queries value:
explorer\main\featurecontrol\feature_protocol_lockdown[unsecapp.exe]
 Queries value:
                          HKLM\system\currentcontrolset\control\wmi\security[981f2d7e-b1f3-11d0-
8dd7-00c04fc3358c]
                           HKLM\system\currentcontrolset\control\wmi\security[981f2d7d-b1f3-11d0-
 Oueries value:
8dd7-00c04fc3358c1
 Sets/Creates value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
 Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[1h6wzb8f9vux2v7xspnwvurp]
 Sets/Creates value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
 Sets/Creates value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1409]
 Sets/Creates value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1409]
 Sets/Creates value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1409]
 Sets/Creates value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1409]
 Sets/Creates value:
                           HKCU\software\microsoft\internet
explorer\phishingfilter[shownservicedownballoon]
 Sets/Creates value:
                           HKCU\software\microsoft\internet
explorer\recovery[clearbrowsinghistoryonexit]
 Sets/Creates value:
                          \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings[globaluseroffline]
 Value changes:
                          HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:
                           HKCU\sessioninformation[programcount]
 Value changes:
                           settings[enablehttp1_1]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
 Value changes:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1609]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1406]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1609]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1406]
 Value changes:
                           \label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet
settings\zones\2[1609]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1406]
                           \label{local-observation} \mbox{HKCU\software\mbox{\tt microsoft\windows\currentversion\internet}} \\
 Value changes:
settings\zones\3[1409]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1609]
 Value changes:
                           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1406]
 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\windows\currentversion\internet settings\lockdown_zones\1[1406] Value changes: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ zones\2[1406] settings\lockdown_ Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones 3[1406] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\lockdown_zones\4[1406] HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8] Value changes: Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[history] Value changes: $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + current version + explorer + shell$ folders[common appdata] Value changes: $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKCU \software \mbox{\mathbb{N} indows \current version \explorer \shell} \\ \end{tabular}$ folders[appdata] Value changes: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ settings[proxyenable] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings\connections[savedlegacysettings] Value changes: HKCU\software\microsoft\windows\currentversion\internet settings[globaluseroffline]

Value changes:

HKLM\system\currentcontrolset\services\eventlog\application\microsoft

h.323 telephony service provider[eventmessagefile]

Value changes: ${\tt HKLM \ } system \verb| current control set \verb| services \verb| eventlog \verb| application \verb| micros of t | application \verb| for the substitution of the sub$

h.323 telephony service provider[typessupported]

Value changes:

HKLM\software\microsoft\wbem\wdm[c:\windows\system32\advapi32.dll[mofresourcename]]