Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 54, Task ID: 216

Task ID: 216 Risk Level:

Date Processed: 2016-04-28 12:53:12 (UTC)

Processing Time: 12.37 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\607c7d18e490c5b56e91c74a29ae3e0a.exe"

Sample ID: Type: basic Owner: admin

607c7d18e490c5b56e91c74a29ae3e0a Label:

2016-04-28 12:44:55 (UTC) Date Added: PE32:win32:gui File Type:

File Size: 106104 bytes

607c7d18e490c5b56e91c74a29ae3e0a MD5:

SHA256: 006257143f3aa20ebc8a51441005feee0cce6d81bca404356d3c1cb657345b9e

Description: None

Pattern Matching Results

3 Long sleep detected

1 HTTP connection - response code 404 (file not found) [HTTP, GET, POST, web, network, response code]

2 PE: Nonstandard section

3 HTTP connection - response code 200 (success) [HTTP, POST, GET, web, network, response code]

4 Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

Anomaly: PE: Contains a virtual section

PE: Contains one or more non-standard sections

Process/Thread Events

C:\windows\temp\607c7d18e490c5b56e91c74a29ae3e0a.exe Creates process:

["C:\windows\temp\607c7d18e490c5b56e91c74a29ae3e0a.exe"]

Terminates process: C:\Windows\Temp\607c7d18e490c5b56e91c74a29ae3e0a.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex Creates mutex: \Sessions\1\BaseNamedObjects_!MSFTHISTORY!_

Creates mutex:

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

files!content.ie5! Creates mutex:

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

Creates mutex:

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

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

 $\verb|\Sessions|1\BaseNamedObjects| RasPbFile| \\$ Creates mutex: Creates mutex: \Sessions\1\BaseNamedObjects\IESQMMUTEX_0_208 \KernelObjects\MaximumCommitCondition Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX Creates event:

\BaseNamedObjects\BFE_Notify_Event_{94e5150b-8784-4f35-b46d-Creates event:

36ebe4a6b542}

File System Events

Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches

Creates: C:\Users\Admin\AppData\Local\Temp\

C:\Users\Admin\AppData\Local\Temp\nsxC731.tmp Creates: Creates: C:\Users\Admin\AppData\Local\Temp\nspC778.tmp C:\Users\Admin\AppData\Local\Temp\nszC783.tmp Creates:

Creates: C:\Users C:\Users\Admin Creates:

C:\Users\Admin\AppData Creates: Creates: C:\Users\Admin\AppData\Local C:\Users\Admin\AppData\Local\Temp Creates:

C:\Users\Admin\AppData\Local\Temp\nszC783.tmp\System.dll Creates: Creates:

C:\Users\Admin\AppData\Local\Temp\28C507DB-D7FB-4AEC-9C80-02EC74BC9D8C Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files Creates:

Creates: C:\Users\Admin\AppData\Roaming

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies Creates: C:\Users\Admin\AppData\Local\Microsoft\Windows\History Creates: Creates:

```
C:\Windows\Prefetch\607C7D18E490C5B56E91C74A29AE3-1B2D8BFB.pf
  Opens:
                                      C:\Windows\System32
  Opens:
  Opens:
                                      C:\Windows\System32\sechost.dll
                                      C:\windows\temp\607c7d18e490c5b56e91c74a29ae3e0a.exe.Local\
  Opens:
  Opens:
                                      C:\Windows\winsxs\x86 microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
  Opens:
                                      C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
  Opens:
                                      C:\windows\temp\VERSION.dll
  Opens:
                                      C:\Windows\System32\version.dll
  Opens:
                                      C:\Windows\System32\imm32.dll
  Opens:
                                      C:\Windows\System32\rpcss.dll
  Opens:
                                      C:\windows\temp\CRYPTBASE.dll
                                      C:\Windows\System32\cryptbase.dll
  Opens:
  Opens:
                                      C:\Windows\System32\uxtheme.dll
  Opens:
                                      C:\windows\temp\SHFOLDER.DLL
  Opens:
                                      C:\Windows\System32\shfolder.dll
  Opens:
                                      C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:
                                      C:\Windows\System32\shell32.dll
  Opens:
                                      C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
                                      C:\Windows\winsxs\x86_microsoft.windows.common-
  Opens:
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
                                      C:\Windows\WindowsShell.Manifest
  Opens:
  Opens:
                                      C:\
  Opens:
                                      C:\Windows
  Opens:
                                      C:\Windows\System32\propsys.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
  Opens:
                                      C:\windows\temp\ntmarta.dll
  Opens:
                                      C:\Windows\System32\ntmarta.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000006.db
  Opens:
                                      C:\Users\Admin\Desktop\desktop.ini
  Opens:
                                      C:\windows\temp\profapi.dll
  Opens:
                                      C:\Windows\System32\profapi.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp
  Opens:
                                      C:\Windows\System32\en-US\setupapi.dll.mui
  Opens:
                                      C: \verb|Vsers\Admin\AppData\Local\Temp\nsxC731.tmp| \\
  Opens:
                                      C:\Windows\Temp\607c7d18e490c5b56e91c74a29ae3e0a.exe
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\nszC783.tmp
                                      C:\Users
  Opens:
  Opens:
                                      C:\Users\Admin
  Opens:
                                      C:\Users\Admin\AppData
                                      C:\Users\Admin\AppData\Local
  Opens:
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\nszC783.tmp\System.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Temp\nszC783.tmp\zplugins.dll
                                      \label{local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-local-loc
  Opens:
  Opens:
                                      C:\Windows\System32\wininet.dll
  Opens:
                                      C:\windows\temp\SspiCli.dll
  Opens:
                                      C:\Windows\System32\sspicli.dll
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\desktop.ini
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
  Opens:
Files\Content.IE5
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
  Opens:
                                      C:\Users\Admin\AppData\Roaming
                                      C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
  Opens:
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
                                      \verb|C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5| \\
  Opens:
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
  Opens:
                                      C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
  Opens:
                                     C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
  Opens:
C:\windows\temp\dnsapi.DLL
  Opens:
  Opens:
                                      C:\Windows\System32\dnsapi.dll
  Opens:
                                      C:\windows\temp\iphlpapi.DLL
  Opens:
                                      C:\Windows\System32\IPHLPAPI.DLL
  Opens:
                                      C:\windows\temp\WINNSI.DLL
  Opens:
                                      C:\Windows\System32\winnsi.dll
  Opens:
                                      C:\windows\temp\RASAPI32.dll
  Opens:
                                      C:\Windows\System32\rasapi32.dll
  Opens:
                                      C:\windows\temp\rasman.dll
  Opens:
                                      C:\Windows\System32\rasman.dll
  Opens:
                                      C:\windows\temp\rtutils.dll
  Opens:
                                      C:\Windows\System32\rtutils.dll
                                      C:\ProgramData\Microsoft\Network\Connections\Pbk\
  Opens:
  Opens:
                                      C:\Windows\System32\ras
```

Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk

Opens: C:\windows\temp\sensapi.dll C:\Windows\System32\SensApi.dll Opens: Opens: C:\Windows\System32\nlaapi.dll Opens: C:\windows\temp\rasadhlp.dll Opens: C:\Windows\System32\rasadhlp.dll C:\Windows\System32\mswsock.dll Opens: C:\Windows\System32\WSHTCPIP.DLL Opens: Opens: C:\Windows\System32\wship6.dll Opens: C:\windows\temp\dhcpcsvc6.DLL Opens: C:\Windows\System32\dhcpcsvc6.dll Opens: C:\windows\temp\dhcpcsvc.DLL Opens: C:\Windows\System32\dhcpcsvc.dll Opens: C:\Windows\System32\drivers\etc\hosts Opens: C:\Windows\System32\FWPUCLNT.DLL Opens: C:\Windows\System32\NapiNSP.dll Opens: C:\Windows\System32\pnrpnsp.dll Opens: C:\Windows\System32\winrnr.dll C:\Windows\System32\netprofm.dll

Opens: C:\Windows\System32\winrnr.dll
Opens: C:\Windows\System32\netprofm.dll
Opens: C:\windows\System32\respected ll
Opens: C:\windows\System32\cryptsp.dll
Opens: C:\windows\System32\rsaenh.dll
Opens: C:\windows\temp\RpcRtRemote.dll
Opens: C:\windows\System32\RpcRtRemote.dll

Opens: C:\Users\Admin\AppData\Local\Temp\28C507DB-D7FB-4AEC-9C80-02EC74BC9D8C

C:\Windows\System32\npmproxy.dll

Writes to: C:\Users\Admin\AppData\Local\Temp\nspC778.tmp

Writes to: C:\Users\Admin\AppData\Local\Temp\nszC783.tmp\System.dll
Writes to: C:\Users\Admin\AppData\Local\Temp\nszC783.tmp\zplugins.dll

Reads from: C:\Users\Admin\Desktop\desktop.ini

Reads from: C:\Windows\Temp\607c7d18e490c5b56e91c74a29ae3e0a.exe
Reads from: C:\Users\Admin\AppData\Local\Temp\nspC778.tmp

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

Deletes: C:\Users\Admin\AppData\Local\Temp\nsxC731.tmp
Deletes: C:\Users\Admin\AppData\Local\Temp\nszC783.tmp

Deletes: C:\Users\Admin\AppData\Local\Temp\nszC783.tmp\result.txt
Deletes: C:\Users\Admin\AppData\Local\Temp\nszC783.tmp\System.dll
Deletes: C:\Users\Admin\AppData\Local\Temp\nszC783.tmp\zplugins.dll

Network Events

Opens:

DNS query: dl.distromatic.com

DNS query: wpad

DNS query: utrack.n.distromatic.com

DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.176$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.19$ $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.221$ DNS response: DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.98$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.39$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.106$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.203$ DNS response: $d2624xgal0u1e4.cloudfront.net \Rightarrow 54.230.144.83$ DNS response: utrack.n.distromatic.com ⇒ 52.87.82.229 DNS response: utrack.n.distromatic.com ⇒ 52.73.93.66

Connects to: 54.230.144.176:80
Connects to: 52.87.82.229:80
Sends data to: 8.8.8.8:53

Sends data to: d2624xgal0u1e4.cloudfront.net:80 (54.230.144.176)

 Sends data to:
 0.0.0.0:5355

 Sends data to:
 224.0.0.252:5355

Sends data to: utrack.n.distromatic.com:80 (52.87.82.229)

Receives data from: 8.8.8.8:53

Receives data from: d2624xgal0u1e4.cloudfront.net:80 (54.230.144.176)

Receives data from: utrack.n.distromatic.com:80 (52.87.82.229)

Windows Registry Events

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

Creates key: HKLM\software\microsoft\tracing

Creates key:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32

Creates key:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs

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

settings\wpad\{280e2f29-0f8b-4d54-9bbd-a14029ca98c2}

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

 $settings \verb|\wpad|{280e2f29-0f8b-4d54-9bbd-a14029ca98c2}\\ \verb|\e2-b5-dc-4d-02-4f| \\$

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

settings\wpad\e2-b5-dc-4d-02-4f 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] Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key: Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key: Opens key: HKLM\software\policies\microsoft\mui\settings HKCU\software\policies\microsoft\control panel\desktop Opens key: Opens key: HKCU\control panel\desktop\languageconfiguration Opens key: HKCU\control panel\desktop Opens key: HKCU\control panel\desktop\muicached Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots HKLM\system\currentcontrolset\control\nls\sorting\versions Opens kev: Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre_initialize$ Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: HKI M\ Opens key: HKLM\software\microsoft\windows nt\currentversion\windows Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics Opens key: HKLM\software\microsoft\ole Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: Opens key: HKLM\software\microsoft\oleaut Opens key: HKCU\software\classes\ Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder Opens key: Opens key: $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-theoryte \} + theoryte \setminus foreign + theoryte \}$ 3aea-1069-a2d8-08002b30309d}\shellfolder Opens key: 3aea-1069-a2d8-08002b30309d}\shellfolder HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens kev: $\label{thm:local_hammon} \parbox{$HKLM\software\microsoft\windows\currentversion\policies\nonenum} \parbox{$honenum$} \parbox$ Opens key: Opens key: 11e3-b3bc-806e6f6e6963}\ HKCU\software\classes\drive\shellex\folderextensions Opens key: Opens key: HKCR\drive\shellex\folderextensions Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9} Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9} Opens key: HKLM\software\policies\microsoft\windows\explorer Opens key: HKCU\software\policies\microsoft\windows\explorer Opens key: HKCU\software\microsoft\windows\currentversion\explorer HKCU\software\microsoft\windows\currentversion\explorer\ Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: $HKLM \label{lem:hklm} Software \verb|\microsoft| windows \verb|\shell| registered applications \verb|\urlassociations| directory \verb|\openwithprogids| and the lemma of the l$

Opens key:

HKCU\software\microsoft\windows\shell\associations\urlassociations\directory

HKCU\software\classes\directory Opens key:

Opens key: HKCR\directory

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

Opens key:

Opens key: HKCR\directory\

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

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

Opens key: HKCR\folder

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

Opens key: HKCR\folder\shellex\iconhandler

HKCU\software\classes\allfilesystemobjects Opens kev:

Opens key: HKCR\allfilesystemobjects

```
HKCU\software\classes\allfilesystemobjects\shellex\iconhandler
     Opens key:
                                                                            HKCR\allfilesystemobjects\shellex\iconhandler
     Opens key:
     Opens kev:
                                                                            HKCU\software\classes\directory\docobject
     Opens key:
                                                                            HKCR\directory\docobject
     Opens key:
                                                                            HKCU\software\classes\folder\docobject
     Opens key:
                                                                            HKCR\folder\docobject
                                                                            HKCU\software\classes\allfilesystemobjects\docobject
     Opens key:
                                                                            HKCR\allfilesystemobjects\docobject
     Opens key:
     Opens key:
                                                                            HKCU\software\classes\directory\browseinplace
     Opens key:
                                                                            HKCR\directory\browseinplace
                                                                            HKCU\software\classes\folder\browseinplace
     Opens key:
     Opens key:
                                                                            HKCR\folder\browseinplace
     Opens key:
                                                                            HKCU\software\classes\allfilesystemobjects\browseinplace
     Opens key:
                                                                            HKCR\allfilesystemobjects\browseinplace
     Opens key:
                                                                            HKCU\software\classes\directory\clsid
     Opens key:
                                                                            HKCR\directory\clsid
                                                                            HKCU\software\classes\folder\clsid
     Opens kev:
     Opens key:
                                                                            HKCR\folder\clsid
     Opens key:
                                                                            HKCU\software\classes\allfilesystemobjects\clsid
     Opens key:
                                                                            {\tt HKCR\allfilesystemobjects\clsid}
     Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
     Opens kev:
b029-7fe99a87c641}
     Opens key:
b029-7fe99a87c641}\propertybag
                                                                           HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
     Opens key:
     Opens key:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current \lor version \setminus explorer \setminus session in folders
     Opens key:
                                                                           HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders
     Opens key:
                                                                            HKLM\software\microsoft\com3
                                                                           HKCU \setminus software \setminus classes \setminus clsid \setminus \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}
     Opens key:
     Opens key:
                                                                            HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
     Opens key:
                                                                            HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\treatas
                                                                            HKCR\clsid{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
     Opens key:
     Opens key:
                                                                            HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d\progid
                                                                            HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid
     Opens key:
                                                                           HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
     Opens kev:
b8dc300d9f9d\inprocserver32
                                                                            HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32
     Opens kev:
                                                                            HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
     Opens key:
b8dc300d9f9d}\inprochandler32
     Opens key:
                                                                            HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\) in prochandler 32
                                                                           HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-
     Opens kev:
b8dc300d9f9d}\inprochandler
                                                                           HKCR \verb|\clsid|{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} \verb|\inprochandler| \\
     Opens key:
     Opens key:
                                                                            HKLM\system\currentcontrolset\control\lsa\accessproviders
     Opens key:
                                                                           HKLM\system\currentcontrolset\services\ldap
     Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
     Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-
b4ef-bd1dc332aeae}
     Opens key:
HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-4786-b587-47
b4ef-bd1dc332aeae}\propertybag
     Opens key:
a03a-e3ef65729f3d}
     Opens key:
HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '{3}eb685db-65f9-4cf6-eps \ 'explorer' \ 'explorer'' \ 'explorer' \ 'explorer'' \ 
a03a-e3ef65729f3d}\propertybag
     Opens key:
HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \ \{5e6c858f-0e22-4760-164e4464, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-19980000, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997-1998, 1997
9afe-ea3317b67173}
     Opens key:
HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1260 \ 'explorer' \ 'folder descriptions' \ 'folder de
9afe-ea3317b67173}\propertybag
     Opens key:
                                                                           HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 2160590473-689474908-1361669368-1002
     Opens kev:
                                                                           HKLM\svstem\currentcontrolset\control\cmf\config
     Opens key:
                                                                           HKLM\software\microsoft\windows\windows error reporting\wmr
                                                                            HKLM\software\microsoft\windows\currentversion\setup
     Opens key:
```

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

Opens key:

Opens key: HKLM\svstem\setup

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

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

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

Opens key:

11e3-b3bc-806e6f6e6963}\

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

Opens key:

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

options\dllnxoptions

Opens key: HKLM\system\currentcontrolset\services\crypt32

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

settings

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

settings

Opens key:

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

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

HKLM\software

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

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

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

settings\5.0\cache

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

settings\5.0\cache

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

settings\5.0\cache\content

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

settings\5.0\cache\content

Opens kev:

ba85-6007caedcf9d}

Opens key:

ba85-6007caedcf9d}\propertybag

Opens kev:

9d55-7b8e7f157091}

Opens key:

9d55-7b8e7f157091}\propertybag

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

settings\5.0\cache\cookies

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

settings\5.0\cache\cookies

Opens key:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ `folder descriptions \ `\{2b0f765d-c0e9-4171-descriptions \ `explorer \ `folder descriptions \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `folder \ `explorer \ `explorer \ `folder \ `explorer \ `ex$ 908e-08a611b84ff6}

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}\propertybag

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

settings\5.0\cache\history

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

settings\5.0\cache\history

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432ea781-5a1130a75963}

Opens kev:

a781-5a1130a75963}\propertybag

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

settings\5.0\cache\extensible cache

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

settings\5.0\cache\extensible cache\domstore

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

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

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

 $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \cite{thm:lem:hkcu} in terms to the lemma substitution \cite{thm:lem:hkcu} and \cite{thm:lem:hkcu} are \cite{thm:lem:hkcu}.$ settings\5.0\cache\extensible cache\ietld

Opens key:

HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\privacie:

Opens key: HKCU\software\microsoft\internet

explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset

Opens key: HKCU\software\microsoft\internet

```
explorer\main\featurecontrol\feature_bufferbreaking_818408
                       HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_bufferbreaking_818408
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
                       HKLM\software\policies\microsoft\windows\currentversion\internet
 Opens kev:
settings\5.0\cache
 Opens key:
                       HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
                       HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_allow_long_international_filenames
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
                       HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
                       HKLM\software\microsoft\internet
 Opens key:
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_exclude_invalid_client_cert_kb929477
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
 Opens key:
                       HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
                       HKCU\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
                       HKLM\software\microsoft\internet
 Opens key:
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
 Opens key:
                       HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
                       HKLM\software\microsoft\internet
 Opens kev:
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
 Opens key:
                       HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:
                       HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\00f84a46
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
 Opens key:
Opens kev:
```

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \000000000011 \parameters \end{substitute} Opens key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
Opens kev:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \0000000000013 \parameters \end{substitute} Opens key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
Opens key:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \0000000000017 \parameters \end{substitute} Opens key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

Opens key:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \00000000c \normal opens key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:

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

Opens key: HKCU\software\microsoft\internet

HKCU\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

Opens key: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_http_username_password_disable

Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209

Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_include_port_in_spn_kb908209

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

 $\verb|explorer\main\featurecontrol\feature_mime_handling| \\$

Opens key:

Opens key:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32

Opens key:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\system\currentcontrol\sqmservicelist

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

Opens key: HKU\

Opens key: HKCU\software\classes\autoproxytypes

Opens key: HKCR\autoproxytypes

Opens key: HKCU\software\classes\autoproxytypes\application/x-internet-signup

Opens key: HKCR\autoproxytypes\application/x-internet-signup

Opens key: HKCU\software\classes\autoproxytypes\application/x-ns-proxy-autoconfig

Opens key: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient

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

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock

Opens key: HKLM\system\currentcontrolset\services\psched\parameters\winsock

Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers

Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\psched

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

Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip

Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip6

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

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

Opens key:

c19ce8a73253}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-

c19ce8a73253} Opens key:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-

806e6f6e6963} Opens key:

806e6f6e6963} Opens key:

1709a0196aed} Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-

a68f334c8d34}

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

Opens key: HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}

Opens key: HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
Opens key: HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-

199fdba5723b}\treatas

Opens key: HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\treatas
Opens key: HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-

199fdba5723b}\progid

Opens key: HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\progid Opens key: HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-

199fdba5723b}\inprocserver32

Opens key: $\label{linear_equation} \mbox{HKCR\clsid\dcb00c01-570f-4a9b-8d69-199fdba5723b} \mbox{inprocserver32}$

Opens key: HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-

199fdba5723b}\inprochandler32

 $Opens~key: \\ HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\\\ inprochandler 32$

Opens key: HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-

199fdba5723b}\inprochandler

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

Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}

Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-

 $001185ad2b89 \} \verb|\treatas|$

001185ad2b89}\progid

Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-

001185ad2b89}\inprocserver32

Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprocserver32

Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-

001185ad2b89}\inprochandler32

Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler32

Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-

001185ad2b89}\inprochandler

Opens key: $\label{eq:hkkcr} \begin{tabular}{ll} HKCR\clsid\a47979d2-c419-l1d9-a5b4-001185ad2b89\inprochandler \\ Opens key: \\ HKCU\software\classes\appid\607c7d18e490c5b56e91c74a29ae3e0a.exe \\ \end{tabular}$

Opens key: HKCR\appid\607c7d18e490c5b56e91c74a29ae3e0a.exe

Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\system\currentcontrol\set\control\lsa

 $Opens\ key: \\ HKLM\software\microsoft\cryptography\defaults\provider\microsoft\ strong$

cryptographic provider

Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy

Opens key:

 $\label{thm:local_policies} \textbf{HKLM} \ system \ \texttt{current} control set \\ \texttt{policies} \ \texttt{microsoft} \ \texttt{cryptography} \\ \texttt{configuration} \\$

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

Opens key: HKLM\software\microsoft\cryptography

Opens key: HKLM\software\microsoft\cryptography\offload

Opens key: HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}

000000000046}\proxystubclsid32

Opens key: HKCR\interface\{00000134-0000-0000-0000-00000000046}\proxystubclsid32

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

Opens key: HKCU\software\classes\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}

HKCR\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b} Opens kev: Opens key: HKCU\software\classes\interface\{d0074ffd-570f-4a9b-8d69-

199fdba5723b}\proxystubclsid32

Opens key: $HKCR \land face \land \{d0074ffd-570f-4a9b-8d69-199fdba5723b\} \land proxystubclsid32$ $HKCU \setminus software \setminus classes \setminus clsid \setminus \{1299cf18-c4f5-4b6a-bb0f-2299f0398e27\}$ Opens key:

Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27} HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-Opens key:

2299f0398e27}\treatas

Opens kev: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-

2299f0398e27}\progid

HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid Opens key: Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-

2299f0398e27}\inprocserver32

Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32

Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-

2299f0398e27}\inprochandler32

HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler32 Opens key:

Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-

2299f0398e27}\inprochandler

 $HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\ \ in prochandler$ Opens kev: Opens key: HKCU\software\classes\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}

Opens key: HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406} Opens key: HKCU\software\classes\interface\{26656eaa-54eb-4e6f-8f85-

4f0ef901a406}\proxystubclsid32

Opens key: $HKCR\interface \ \{26656eaa-54eb-4e6f-8f85-4f0ef901a406\} \ proxystubclsid 32$ Opens key: HKCU\software\classes\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}

Opens key: HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec} Opens key: HKCU\software\classes\interface\{8a40a45d-055c-4b62-abd7-

6d613e2ceaec}\proxystubclsid32

Opens key: $HKCR \land 13e2 ceaec \rbrace \land 13e2 ceaec \rbrace$ Opens key: HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-00aa004bb851}

HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851} Opens kev: Opens key: HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-

00aa004bb851}\proxystubclsid32

 $HKCR \verb|\interface| \{55272a00-42cb-11ce-8135-00aa004bb851\} \verb|\proxystubclsid32| \} where $(55272a00-42cb-11ce-8135-00aa004bb851) | $(55272a0a0-42cb-11ce-8135-00aa004bb851) | $(55272a0a0-42cb-11ce-8135-00aa004bb851) | $(55272a0a0-42cb-11ce-8135-00aa004bb851) | $(55272a0a0-42cb-11ce-8135-00aa004bb851) | $(55272a0a0-42cb-11ce-8135-00aa004bb851) | $(55272a0a0-42cb-11ce-8135-00aa004bb851) | $(55272a0a0-42cb-11ce-8135-00aa004b851) | $(55272a0a0-42cb-11ce-8135-00aa004b851) | $(55272a0a0-42cb-11ce-8135-00aa004b851) | $(55272a0a0-42cb-11ce-8135-00aa004b851) | $(55272a0a0-42cb-11ce-8135-00aa004b851) | $(55272a0a0-42cb-11$ Opens key: Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}

Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07} Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-

00aa00341d07}\treatas Opens key:

HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-Opens key: 00aa00341d07}\progid

Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-Opens key:

00aa00341d07}\inprocserver32

HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-

00aa00341d07}\inprochandler32

HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler32 Opens key:

Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-

00aa00341d07}\inprochandler

Opens kev: $HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\$ inprochandler $HKCU \setminus software \setminus classes \setminus interface \setminus \{bcd1de7e-2db1-418b-b047-4a74e101f8c1\}$ Opens key:

Opens key: HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1} Opens key: HKCU\software\classes\interface\{bcd1de7e-2db1-418b-b047-

4a74e101f8c1}\proxystubclsid32

Opens key: $HKCR \land terface \land \{bcd1de7e-2db1-418b-b047-4a74e101f8c1\} \land proxystubclsid32\}$ Opens key: HKCU\software\classes\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}

HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037} Opens key: Opens key: HKCU\software\classes\interface\{2a1c9eb2-df62-4154-b800-

63278fcb8037}\proxystubclsid32

HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32 Opens key:

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

settings\wpad\{280e2f29-0f8b-4d54-9bbd-a14029ca98c2}

Opens key: HKLM\system\currentcontrolset\services\netbt\linkage Queries value: HKLM\system\currentcontrolset\control\session

manager[cwdillegalindllsearch]

Oueries value:

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

Oueries value: HKCU\control panel\desktop[preferreduilanguages]

HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Oueries value:

Queries value:

 $HKLM \verb|\software\microsoft\windows \verb|\currentversion\side| preferex ternal manifest| \\$ $\label{lem:hklm} \verb+Kklm \system \current control set \control \nls \sorting \versions[]$ Queries value:

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

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

nt\currentversion\compatibility32[607c7d18e490c5b56e91c74a29ae3e0a]

Queries value: HKLM\software\microsoft\windows

```
nt\currentversion\windows[loadappinit_dlls]
                                                   HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Oueries value:
   Oueries value:
                                                   HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
                                                   HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Queries value:
                                                   HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Oueries value:
   Queries value:
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[attributes]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[callforattributes]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[restrictedattributes]
   Queries value:
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsfordisplay]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[hidefolderverbs]
   Queries value:
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[usedrophandler]
   Queries value:
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsforparsing]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[wantsparsedisplayname]
   Queries value:
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[queryforinfotip]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hideinwebview]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
   Queries value:
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[nofilefolderjunction]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Oueries value:
08002b30309d}\shellfolder[pintonamespacetree]
                                                   HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
   Queries value:
08002b30309d}\shellfolder[hasnavigationenum]
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus monenum [\{20d04fe0-3aea-1069-a2d8-microsoft\}] + (20d04fe0-3aea-1069-a2d8-microsoft) + (20d04fe0-3aea-1069-a2d8-mi
08002b30309d}1
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{69d250e4-6c18-
11e3-b3bc-806e6f6e6963}[data]
11e3-b3bc-806e6f6e6963}[generation]
   Oueries value:
                                                   HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask1
   Queries value:
                                                   HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Queries value:
                                                   \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\advanced[hidden]| \\ \end{tabular}
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   Oueries value:
\label{thm:local_explorer_ladvanced} HKCU \software \microsoft \windows \current version \explorer \advanced \[dont pretty path] \\
   Queries value:
\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} is a constant \cite{tabular} and \cite{tabular
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
   Queries value:
                                                   \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced [filter] \end{tabular}
   Oueries value:
HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced [shows uper hidden]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
   Queries value:
Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
                                                   HKCR\directory[docobject]
   Oueries value:
   Queries value:
                                                   HKCR\folder[docobject]
```

Queries value: HKCR\allfilesystemobjects[docobject] HKCR\directory[browseinplace] Oueries value:

Oueries value: HKCR\folder[browseinplace]

Queries value: HKCR\allfilesystemobjects[browseinplace]

Oueries value: HKCR\directory[isshortcut] Queries value: HKCR\folder[isshortcut]

Oueries value: HKCR\allfilesystemobjects[isshortcut]

Oueries value: HKCR\directory[alwaysshowext] Queries value: HKCR\directory[nevershowext] Queries value: HKCR\folder[nevershowext]

Oueries value: HKCR\allfilesystemobjects[nevershowext]

Queries value:

b029-7fe99a87c641}[category]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[name]

Queries value:

b029-7fe99a87c641}[parentfolder]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[description]

b029-7fe99a87c641}[relativepath]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[parsingname]

b029-7fe99a87c641}[infotip]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[localizedname]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[icon]

Queries value:

b029-7fe99a87c641}[security]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[streamresource]

Oueries value:

b029-7fe99a87c641}[streamresourcetype]

Queries value:

b029-7fe99a87c641}[localredirectonly]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[roamable]

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[precreate]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[stream]

b029-7fe99a87c641}[publishexpandedpath]

Queries value:

b029-7fe99a87c641}[attributes]

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424cb029-7fe99a87c641}[foldertypeid]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ (b4bfcc3a-db2c-424c-db2c-42b) \ descriptions \ (b4bfcc3a-db2c-424c-db2c-42b) \ descriptions \ de$ b029-7fe99a87c641}[initfolderhandler]

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

folders[desktop]

Queries value: HKLM\software\microsoft\com3[com+enabled]

Queries value: $HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\}[]$

Oueries value: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[inprocserver32]

HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\inprocserver32[] Oueries value:

Oueries value: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[threadingmodel]

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

Oueries value:

 $HKLM \setminus system \setminus current control \setminus lsa \setminus access providers [martaextension]$

Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value: HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]

 $\label{thm:current} Queries \ value: \\ HKLM \ system \ current control set \ services \ ldap [use host name as a lias] \\$

Queries value:

 $HKLM \ software \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ [category]$

Queries value:

 $HKLM \ software \ `microsoft \ 'unidows \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [name]$

Queries value:

 $HKLM \ software \ `microsoft \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ [parent folder]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [description]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [relative path]$

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parsingname]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ 'infotip' \ 'explorer' \ 'explorer'' \ 'explorer' \ 'explore$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [localized name]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ [icon]$

Oueries value:

 $\label{local-basis} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[security]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [stream resource]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [stream resource type]$

Queries value:

 $HKLM\software\mbox{$1b3ea5dc-b587-4786-b4ef-bd1dc332aeae} [localredirectonly] \\$

Queries value:

 $HKLM \ software \ `microsoft \ 'urrent version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ [roamable]$

Queries value:

 $\label{local-basis} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[precreate]$

Queries value:

 $HKLM \ software \ `microsoft \ 'urrent version \ 'explorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [stream]$

Oueries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} In the sum of the label of the sum of the sum$

Queries value:

 $\label{lem:hamman} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[attributes]$

Queries value:

Queries value:

 $HKLM \ software \ `microsoft \ 'unidows \ 'current version \ 's plorer \ 'folder descriptions \ '\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [initfolder \ handler]$

Queries value: $HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]$

Queries value

 $\label{lem:hkkm} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \calebox{3eb685db-65f9-4cf6-a03a-e3ef65729f3d} \category\cite{Control of the control of the control$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[name]$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescriptions\folderdescriptions\folderdescription\folderdescriptio$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[parsingname]}$

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\folder$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[localized name]}$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[icon]$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} In the constant of the constant of$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[streamresource]$

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ 'abb685 db-65 f9-4c f6-a03a-e3e f65 729 f3d \ [local redirect only]$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[roamable]$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[precreate]$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[stream]}$

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[initfolderhandler]$

Queries value:

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

folders[appdata]

Oueries value:

 $\label{thm:local-prop} $$HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[category]$$$

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'entre \ 'entre$

Queries value:

 $\label{thm:local-problem} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[description]}$

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[relativepath]}$

Queries value:

 $\label{thm:local-prop} $HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[parsingname]} $$$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[infotip]} Infotip \[\] $$ (a) $$ (a) $$ (a) $$ (b) $$ (b) $$ (b) $$ (c) $$

Queries value:

 $\label{thm:microsoft} $HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions \{5e6c858f-0e22-4760-9afe-ea3317b67173\}[localized name] $$$

Queries value:

 $HKLM \ software \ `microsoft \ 'enclosed \ 'enclosed$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[streamresource]}$

Queries value:

 $\label{thm:local-prop} $HKLM \sim \min(s) - 1.00$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[localredirectonly]}$

```
Oueries value:
```

9afe-ea3317b67173}[roamable]

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{5e6c858f-0e22-4760-1640-16400-164$ 9afe-ea3317b67173}[precreate]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]

Oueries value:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ folder descriptions \ `\{5e6c858f-0e22-4760-1640-16400-164$ 9afe-ea3317b67173}[publishexpandedpath]

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]

Oueries value:

 $HKLM \setminus software \setminus irrosoft \setminus ir$ 9afe-ea3317b67173}[foldertypeid]

Queries value:

9afe-ea3317b67173}[initfolderhandler]

HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-Oueries value:

2160590473-689474908-1361669368-1002[profileimagepath]

HKLM\system\currentcontrolset\control\cmf\config[system] Queries value:

Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable] HKLM\software\microsoft\windows\currentversion\setup[sourcepath] Queries value: Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]

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

Oueries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\setup[oobeinprogress] HKLM\system\setup[systemsetupinprogress] Queries value:

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

Queries value:

11e3-b3bc-806e6f6e6963}[data]

Oueries value:

11e3-b3bc-806e6f6e6963}[generation]

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter]

HKLM\software\microsoft\windows nt\currentversion\image file execution Queries value:

options\dllnxoptions[system.dll]

Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags] HKLM\software\microsoft\windows\currentversion\internet Oueries value:

settings[disableimprovedzonecheck]

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

settings[security_hklm_only] Oueries value:

HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440da3fe-553973d0b7231

Oueries value:

HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796b924-d51178a59ce41

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

settings[fromcachetimeout] HKLM\software\policies\microsoft\windows\currentversion\internet

Oueries value:

settings[secureprotocols] $\label{lem:hkcu} \mbox{\tt HKCU\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu} \mbox{\tt hkcu\software\policies\mbox{\tt microsoft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\linearing}} \mbox{\tt linearing\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\windows\currentversion\color=lem:hkcu\soft\color=lem:hkcu$ Queries value:

settings[secureprotocols]

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

settings[secureprotocols]

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

settings[certificaterevocation]

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

settings[disablekeepalive]

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

settings[disablepassport]

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

settings[idnenabled]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[cachemode]

Queries value:

HKLM\software\policies\microsoft\windows\currentversion\internet settings[enablehttp1_1]

Oueries value: settings[enablehttp1_1]

HKCU\software\policies\microsoft\windows\currentversion\internet

Queries value:

HKCU\software\microsoft\windows\currentversion\internet

settings[enablehttp1_1] Queries value:

Oueries value:

HKLM\software\policies\microsoft\windows\currentversion\internet

settings[proxyhttp1.1]

HKCU\software\policies\microsoft\windows\currentversion\internet

settings[proxyhttp1.1]

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

settings[proxyhttp1.1]

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

settings[enablenegotiate] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[disablebasicoverclearchannel] Queries value: HKCU\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol[feature_clientauthcertfilter] Oueries value: HKCU\software\microsoft\windows\currentversion\internet settings[clientauthbuiltinui] Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[syncmode5] Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache[sessionstarttimedefaultdeltasecs] $\label{lem:hkcu} \verb+KCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value: settings\5.0\cache[signature] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\content[peruseritem] HKLM\software\microsoft\windows\currentversion\internet Queries value: settings\5.0\cache\content[peruseritem] Queries value: ba85-6007caedcf9d}[category] Oueries value: ba85-6007caedcf9d}[name] Queries value: ba85-6007caedcf9d}[parentfolder] Oueries value: ba85-6007caedcf9d}[description] Queries value: ba85-6007caedcf9d}[relativepath] Oueries value: ba85-6007caedcf9d}[parsingname] Oueries value: ba85-6007caedcf9d}[infotip] Queries value: ba85-6007caedcf9d}[localizedname] Queries value: ba85-6007caedcf9d}[icon] Queries value: ba85-6007caedcf9d}[security] Queries value: ba85-6007caedcf9d}[streamresource] Queries value: ba85-6007caedcf9d}[streamresourcetype] Queries value: ba85-6007caedcf9d}[localredirectonly] Oueries value: ba85-6007caedcf9d}[roamable] Oueries value: ba85-6007caedcf9d}[precreate] Oueries value: ba85-6007caedcf9d}[stream] Queries value: ba85-6007caedcf9d}[publishexpandedpath] Queries value:

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

Queries value:

ba85-6007caedcf9d}[foldertypeid]

Queries value:

ba85-6007caedcf9d}[initfolderhandler]

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

folders[cache]

Oueries value:

9d55-7b8e7f157091}[category]

Oueries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [parent folder]$

Oueries value:

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

Oueries value:

 $HKLM \ software \ `microsoft \ 'entre \ 'entre$

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \fill 157091 \end{figure} folder \descriptions \fill 157091 \end{figure} fold 157091 \end{figure} fold$

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ folder \ director \ local redirector \ local redirector \ local redirector \ local \ redirector \ local \$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} current version \end{fersions} {f1b32785-6fba-4fcf-9d55-7b8e7f157091} [precreate]$

Queries value:

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}Fpublishexpandedpath1

Queries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [attributes]$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} current version \end{fersions \fib32785-6 fba-4 fcf-9 d55-7 b8e7 f157091} [folder type id]$

Queries value:

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

Queries value:

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

folders[local appdata]

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

settings\5.0\cache\content[cacheprefix]

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

settings\5.0\cache\content[cachelimit]

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

settings\5.0\cache\cookies[peruseritem]

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

settings\5.0\cache\cookies[peruseritem]

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [parent folder]$

Queries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'endows \ 'en$

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \current version \explorer \folder descriptions \current version \explorer \folder descriptions \current version \explorer \folder \folder \folder \current \curren$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[security]}$

Oueries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [stream resource]$

Oueries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [stream resource type]$

Queries value:

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

Queries value:

 $HKLM \software \microsoft \windows \current version \explorer \folder descriptions \current \current$

Queries value:

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

Oueries value:

Queries value:

 $HKLM \ software \ `microsoft \ 'current version \ 'explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [publish expanded path]$

Oueries value:

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

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6\}[foldertypeid]}$

Queries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{2b0f765d-c0e9-4171-908e-08a611b84ff6\} [initfolder \ handler]$

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

folders[cookies]

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

settings\5.0\cache\cookies[cacheprefix]

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

settings\5.0\cache\cookies[cachelimit]

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

settings\5.0\cache\history[peruseritem]

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

settings\5.0\cache\history[peruseritem]

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}\category\cite{Acceptable} and the second se$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [name]$

Oueries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963}[parentfolder]

Queries value:

 $\label{local-bound} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-a781-5a1130a75963\}\[description]\]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ (d9dc8a3b-b784-432e-a781-5a1130a75963) \ [relative path]$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} In the constant of the constant of$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [infotip]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [localized name]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d9dc8a3b-b784-432e-a781-5a1130a75963\} \ [icon]$

```
a781-5a1130a75963}[security]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[streamresource]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[streamresourcetype]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[localredirectonly]
   Queries value:
a781-5a1130a75963}[roamable]
   Queries value:
a781-5a1130a75963}[precreate]
a781-5a1130a75963}[stream]
   Queries value:
a781-5a1130a75963}[publishexpandedpath]
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\{d9dc8a3b-b784-432e-d74b, d9dc8a3b-b784-432e-d74b, d9dc8a5b-b784-432e-d74b, d9dc8a5b-b784-430e-d74b, d9dc8a5b-b784-430e-d74b, d9dc8a5b-b784-430e-d7
a781-5a1130a75963}[attributes]
   Queries value:
a781-5a1130a75963}[foldertypeid]
HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a3b-b784-432e-d9dc8a4b-b784-432e-d9dc8a4b-b784-432e-d9dc8a400-d9dc8a4b-b784-4360-d9dc8a4b-b784-4360-d9dc8a4b-b784-4360-d9dc
a781-5a1130a75963}[initfolderhandler]
                                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
   Queries value:
folders[history]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
                                             HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\history[cachelimit]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
   Queries value:
                                             \label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\linear}} \mbox{\tt internet}
settings\5.0\cache\extensible cache\domstore[cachepath]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\domstore[cacheprefix]
   Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
   Queries value:
                                             \label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\
settings\5.0\cache\extensible cache\domstore[cacheoptions]
                                            \label{lem:hkcu} \verb+KCU\+ software\+ microsoft\+ windows\+ current version\+ internet
  Oueries value:
settings\5.0\cache\extensible cache\feedplat[cacherepair]
   Oueries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\feedplat[cachelimit]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
   Queries value:
                                             settings\5.0\cache\extensible cache\iecompat[cacherepair]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cachepath]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
   Queries value:
                                             HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Queries value:
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
   Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
   Queries value:
                                             settings\5.0\cache\extensible cache\ietld[cachepath]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
settings\5.0\cache\extensible cache\ietld[cacheprefix]
   Queries value:
                                            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
                                             HKCU\software\microsoft\windows\currentversion\internet
   Queries value:
settings\5.0\cache\extensible cache\ietld[cacheoptions]
                                            HKCU\software\microsoft\windows\currentversion\internet
  Oueries value:
```

settings\5.0\cache\extensible cache\privacie:[cacherepair]

settings\5.0\cache\extensible cache\privacie:[cachepath]

HKCU\software\microsoft\windows\currentversion\internet

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

Queries value:

```
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache\extensible cache\privacie:[cachelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
 Oueries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
 Queries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
 Queries value:
                          \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \current version \end{tabular} in termet \end{tabular}
settings[mbcsapiforcrack]
                          HKCU\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[utf8servernameres]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[disableworkerthreadhibernation]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablereadrange]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketsendbufferlength]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[socketreceivebufferlength]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[keepalivetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxhttpredirects]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsperserver]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1_0server]
                          HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[maxconnectionsper1 Oserver]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[serverinfotimeout]
 Queries 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
 Queries value:
settings[connectretries]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
                          HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[sendtimeout]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
 Queries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[disablentlmpreauth]
                          HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[scavengecachelowerbound]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings\5.0\cache[scavengecachefilelifetime]
 Oueries value:
                          HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
 Queries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
                          HKLM\software\microsoft\internet
 Oueries value:
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[607c7d18e490c5b56e91c74a29ae3e0a.exe]
 Oueries value:
                          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature disable unicode handle closing callback[*1
 Oueries value:
                          HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
                          HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[perusercookies]
```

```
Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dialupuselansettings]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[sendextracrlf]
                           \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+\internet+
 Queries value:
settings[wpadsearchalldomains]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasshttpnocachecheck]
                           HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet
 Queries value:
settings[bypasshttpnocachecheck]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[bypasssslnocachecheck]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[bypasssslnocachecheck]
                           HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus internet
 Queries value:
settings[enablehttptrace]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[nocheckautodialoverride]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[nocheckautodialoverride]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
                           HKLM\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dontusednsloadbalancing]
 Queries value:
                           HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[mimeexclusionlistforcache]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[dnscacheentries]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[dnscachetimeout]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
                           HKCU\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[warnalwaysonpost]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
 Queries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
 Oueries value:
                           HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
                           HKCU\software\microsoft\windows\currentversion\internet
 Queries value:
settings[warnonhttpstohttpredirect]
                           HKLM\software\microsoft\windows\currentversion\internet
 Oueries value:
settings[tcpautotuning]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock registry version]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 [next\_catalog\_entry\_id]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 000000000001 \ [packed catalog item]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000005[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
```

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 0000000000007 \ [packed catalog item]$

Oueries value:

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[providerid]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[displaystring]
 Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ name space_catalog \ name space$

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace] Oueries value:

Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[storesserviceclassinfo] Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog 5 \setminus catalog_entries \setminus 0000000000004 [provider info]$ Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace _catalog5 \ catalog_entries \ 00000000005 [library path]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring] Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap amespace_catalog \\ S \setminus catalog_entries \setminus 0000000000005[providerid]$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ (catalog_entries \ 0000000000005 \ [address family]$ Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled] Queries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[storesserviceclassinfo] Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog \\ \setminus catalog_entries \setminus 0000000000005[provider info]$ Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace _catalog5 \ catalog_entries \ 000000000006 [library path]$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000006[displaystring] Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000006[supportednamespace] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[enabled] Oueries value:

Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace_catalog_entries \ (00000000006[storesserviceclass info]) \ (control set \ namespace_catalog \ namespace_catalog_entries) \ (control set \ n$ Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2 32spincount1

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

settings\wpad[wpadoverride] Oueries value: HKCU\software\microsoft\windows\currentversion\internet

settings[enableautodial]

Queries value:

settings[nonetautodial]

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

settings[globaluseroffline] HKCU\software\microsoft\windows\currentversion\internet Queries value:

settings[badproxyexpirestime]

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

settings[disablebranchcache]

HKLM\software\microsoft\internet Queries value:

explorer\main\featurecontrol\feature_http_username_password_disable[607c7d18e490c5b56e91c74a29ae3e0a.exe]

HKCU\software\microsoft\windows\currentversion\internet

HKLM\software\microsoft\internet Queries value:

explorer\main\featurecontrol\feature_http_username_password_disable[*]

Queries value: HKLM\software\microsoft\internet

explorer\main\featurecontrol\feature_mime_handling[607c7d18e490c5b56e91c74a29ae3e0a.exe]

Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature mime handling[*]

HKLM\software\microsoft\tracing[enableconsoletracing] Oueries value:

Oueries value:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[enablefiletracing] Oueries value:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[filetracingmask]

Oueries value:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[enableconsoletracing]

Oueries value:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[consoletracingmask]

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus tracing \setminus 607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[maxfilesize]$

Oueries value: HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[filedirectory] Oueries value: HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[enablefiletracing] Oueries value: HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[filetracingmask] Oueries value: HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[enableconsoletracing] Oueries value: HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[consoletracingmask] Oueries value: HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[maxfilesize] Oueries value: HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[filedirectory] HKLM\software\microsoft\windows Queries value: nt\currentversion\profilelist[programdata] HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist] Oueries value: Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[54f8338f] Queries value: HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling] Queries value: HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession] HKLM\software\policies\microsoft\windows\currentversion\internet Oueries value: settings[proxysettingsperuser] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[migrateproxy] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyenable] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[proxyserver] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings[proxyoverride] $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$ Queries value: settings[autoconfigurl] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\connections[savedlegacysettings] HKCU\software\microsoft\windows\currentversion\internet Oueries value: settings\connections[defaultconnectionsettings] HKCU\software\microsoft\windows\currentversion\internet Queries value: settings[autoconfigcustomua] ${\tt HKCR} \verb| autoproxytypes \verb| application/x-internet-signup[dllfile]|\\$ Oueries value: HKCR\autoproxytypes\application/x-internet-signup[fileextensions] Queries value: HKCR\autoproxytypes\application/x-internet-signup[default] Oueries value: HKCR\autoproxytypes\application/x-internet-signup[flags] Oueries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[dllfile] Oueries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[fileextensions] Queries value: Queries value: $HKCR \verb| autoproxytypes \verb| application/x-ns-proxy-autoconfig[default]| \\$ Queries value: HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[flags] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel] HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value:

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

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

Oueries value:

```
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
 Oueries value:
                        HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
 Oueries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
 Oueries value:
                        HKLM\svstem\currentcontrolset\services\dnscache\parameters[maxcachesize]
                        HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dnscache \setminus parameters [maxcached sockets]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicastresponder flags]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
 Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
```

Oueries value:

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

Oueries value:

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

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

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

Oueries value:

HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping] Oueries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\psched[winsock 2.0 provider id]

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

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

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

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

Oueries value:

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

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname] HKLM\system\currentcontrolset\services\winsock\setup Oueries value:

migration\providers\tcpip6[winsock 2.0 provider id]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]

HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]

Oueries value:

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

Oueries value:

c19ce8a73253}[searchlist]

Queries value:

c19ce8a73253}[enabledhcp]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-

c19ce8a73253}[registrationenabled]

Queries value:

c19ce8a73253}[registeradaptername] Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17c19ce8a73253}[domain]

Oueries value:

c19ce8a73253}[dhcpdomain]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-

c19ce8a73253}[dhcpv6domain]

Oueries value:

c19ce8a73253}[nameserver]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-

c19ce8a73253}[nameserver]

Oueries value:

c19ce8a73253}[dhcpnameserver]

Queries value:

806e6f6e6963}[enabledhcp]

Oueries value:

806e6f6e6963}[registrationenabled]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registeradaptername]

Oueries value:

806e6f6e6963}[domain]

Oueries value:

806e6f6e6963}[dhcpdomain]

Oueries value:

```
806e6f6e6963}[nameserver]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpnameserver]
   Oueries value:
                                                HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[queryadaptername]
   Oueries value:
c19ce8a73253}[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enablemulticast]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[disabledynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enableadapterdomainnameregistration]
806e6f6e6963}[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[maxnumberofaddressestoregister]
   Queries value:
806e6f6e6963}[enablemulticast]
                                                HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
   Queries value:
   Queries value:
                                                HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}[]
                                                HKCR\clsid\{dcb00c01-570f-4a9b-8d69-
   Oueries value:
199fdba5723b}\inprocserver32[inprocserver32]
                                                HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprocserver32[]
   Queries value:
                                                HKCR\clsid\{dcb00c01-570f-4a9b-8d69-
   Queries value:
199fdba5723b}\inprocserver32[threadingmodel]
                                                HKLM\software\microsoft\rpc\extensions[ndroleextdll]
   Oueries value:
                                                HKCR \ clsid \ \{a47979d2-c419-11d9-a5b4-001185ad2b89\}[]
   Queries value:
                                                HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
   Oueries value:
   Queries value:
                                                HKLM\software\microsoft\ole[defaultaccesspermission]
                                                \label{lem:hklmsystem} \verb| HKLM \rangle is a [everyone includes a nonymous] | \\
   Queries value:
                                                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
   Queries value:
cryptographic provider[type]
   Queries value:
                                                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
                                                HKLM\system\currentcontrolset\control\session
   Oueries value:
manager[safeprocesssearchmode]
   Queries value:
                                                HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
   Queries value:
                                                HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
   Oueries value:
                                                HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
   Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
                                                \label{local-operator} \verb|HKLM\| software\| policies\| microsoft\| cryptography [privatekey lifetimeseconds]| | the context of the context o
   Oueries value:
                                                 HKLM\software\microsoft\cryptography[machineguid]
   Oueries value:
   Queries value:
                                                 HKCR\interface\{00000134-0000-0000-c000-00000000046}\proxystubclsid32[]
   Oueries value:
                                                HKLM\software\microsoft\rpc\extensions[remoterpcdll]
   Queries value:
                                                 HKLM\software\microsoft\ole[maximumallowedallocationsize]
                                                 HKCR \land (d0074ffd-570f-4a9b-8d69-199fdba5723b) \land (d0074ffd-570f-4a9b-8d69-199fdba5725b) \land (d0074ffd-570f-4a9b-8d69-199fdba5725b) \land (d0074ffd-570f-4a9b-8d69-199fdba5725b) \land (d0074ffd-570f-4a9b-8d69-199fdba5725b) \land (d0074ffd-570f-4a9b-8d69-199fdba572b) \land (d0074ffd-570f-4a9b-8d69-199fdba572b) \land (d0074ffd-570f-4a9b-8d69-199fdba572b) \land (d0074ffd-6a9b-8d69-199fdba572b) \land (d0074ffd-6a9b-8d69-199fdba572b) \land (d0074ffd-6a9b-8d69-199fdba572b) \land (d0074ffd-6a9b-8d69-199fdba572b) \land (d0074ffd-6a9b-8d69-199fdba572b) \land (d0074ffd-6a9b-8d69-199fdba572b) \land (d0074ffd-6a9b-8d69-199fdb
   Oueries value:
                                                HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}[]
   Queries value:
                                                HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
   Oueries value:
2299f0398e27}\inprocserver32[inprocserver32]
                                               HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32[]
   Queries value:
   Queries value:
                                                HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-}
2299f0398e27}\inprocserver32[threadingmodel]
                                                HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}\proxystubclsid32[]
   Queries value:
```

HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}\proxystubclsid32[] Oueries value: HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}\proxystubclsid32[] Oueries value: Oueries value: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[] Queries value: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32[inprocserver32]

Queries value: $\label{lem:hkcrclsid} $$ HKCR\clsid_{b196b286-bab4-101a-b69c-00aa00341d07} \in \clsid_{b196b286-bab4-101a-b69c-00aa00341d07} $$ in processor of the context of the context$

HKCR\clsid\{b196b286-bab4-101a-b69c-Queries value:

00aa00341d07}\inprocserver32[threadingmodel]

Queries value: HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}\proxystubclsid32[] HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32[] Queries value:

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

settings\wpad[wpadlastnetwork]

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

settings[autoproxydetecttype]

Queries value: HKLM\system\currentcontrolset\services\netbt\linkage[export]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[1540ff4c-3fd7-4bba-

9938-1d1bf31573a71 Sets/Creates value:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[enablefiletracing]

Sets/Creates value:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[enableconsoletracing] Sets/Creates value:

 $HKLM \setminus software \setminus microsoft \setminus tracing \setminus 607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[filetracing mask]$ Sets/Creates value:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[consoletracingmask] Sets/Creates value:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[maxfilesize] Sets/Creates value:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasapi32[filedirectory] Sets/Creates value:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[enablefiletracing] Sets/Creates value:

 $HKLM \setminus software \setminus microsoft \setminus tracing \setminus 607c7d18e490c5b56e91c74a29ae3e0a_rasmancs \\ [enable consoletracing]$ Sets/Creates value:

 $HKLM \setminus software \setminus microsoft \setminus tracing \setminus 607c7d18e490c5b56e91c74a29ae3e0a_rasmancs \\ [filetracing mask] \\$

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[consoletracingmask] Sets/Creates value:

HKLM\software\microsoft\tracing\607c7d18e490c5b56e91c74a29ae3e0a_rasmancs[maxfilesize] Sets/Creates value:

 $HKLM \setminus software \setminus microsoft \setminus tracing \setminus 607c7d18e490c5b56e91c74a29ae3e0a_rasmancs \\ [filedirectory]$

HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value:

settings\wpad\{280e2f29-0f8b-4d54-9bbd-a14029ca98c2}[wpaddecisionreason]

Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet

settings\wpad\{280e2f29-0f8b-4d54-9bbd-a14029ca98c2}[wpaddecisiontime]

HKCU\software\microsoft\windows\currentversion\internet Sets/Creates value: settings\wpad\{280e2f29-0f8b-4d54-9bbd-a14029ca98c2}[wpaddecision]

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

settings\wpad\{280e2f29-0f8b-4d54-9bbd-a14029ca98c2}[wpadnetworkname]

Sets/Creates value:

settings\wpad\e2-b5-dc-4d-02-4f[wpaddecisionreason] HKCU\software\microsoft\windows\currentversion\internet

Sets/Creates value:

settings\wpad\e2-b5-dc-4d-02-4f[wpaddecisiontime] Sets/Creates value: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}$

settings\wpad\e2-b5-dc-4d-02-4f[wpaddecision]

Value changes:

settings[proxyenable]

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

settings\connections[savedlegacysettings]

Value changes: $\label{lem:hkcu} \verb+KKCU \software \microsoft \windows \current version \current \end{tensor}$

settings\connections[defaultconnectionsettings]

Value changes:

settings\wpad[wpadlastnetwork]

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

settings\wpad\{280e2f29-0f8b-4d54-9bbd-a14029ca98c2}[wpaddecisionreason]

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

settings\wpad\{280e2f29-0f8b-4d54-9bbd-a14029ca98c2}[wpaddecisiontime]

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

settings\wpad\{280e2f29-0f8b-4d54-9bbd-a14029ca98c2}[wpaddecision]

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

settings\wpad\{280e2f29-0f8b-4d54-9bbd-a14029ca98c2}[wpadnetworkname] Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\wpad\e2-b5-dc-4d-02-4f[wpaddecisionreason] Value changes: $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ windows \verb+ current version \verb+ internet+ \\$

settings\wpad\e2-b5-dc-4d-02-4f[wpaddecisiontime]

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

settings\wpad\e2-b5-dc-4d-02-4f[wpaddecision]