



### Verification instructions:

The SHA1 hash of "Check.exe" is a1caf5d125e87cfc933529ca64df127f82302ab . Additionally the program will also compute and output its own executable's SHA1 hash every time it is executed.

Also included is a PGP signature for nsrl\_check.zip. If you wish to verify your copy has not been modified, you can download Nicholas Manka's public key [here](#).

### Usage instructions:

1. Unpack the attached nsrl\_check.zip.
2. Open a terminal as administrator.
3. Navigate to the check.exe file.
  - a. Ex:

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>C:\nsrl_check\nsrl_check\check.exe
```

4. The following instructions should appear:
  - a. Ex:

```
Scan a file, directory tree, or list of file hashes from the NSRL.
MODE      : To scan for files or directories
USAGE     : nsrl_check <File or Directory> [Path to CSU]
MODE      : To check a file containing a list of hashes from another tool
USAGE     : nsrl_check list <File with hashes to check> [CSU]
MODE      : To run a self test
USAGE     : nsrl_check test <SHA1 hash> [CSU]
NOTE      : If a path to a CSU hash list is not provided, the current
NOTE      : directory will be searched.
EXAMPLE1: nsrl_check "C:\Program Files"
EXAMPLE2: nsrl_check "C:\Program Files" Downloads\NSRLFile.zip
EXAMPLE3: nsrl_check list fciv_output.xml Downloads\NSRLFile.txt
EXAMPLE4: nsrl_check test 002AD3BE677F36643D7E3489BD5DC6C1D04A6401
WARNING  : THIS PROGRAM IS RELEASED TO THE PUBLIC DOMAIN AS IS WITH
WARNING  : NO WARRANTY OR GAURANTEE OF USABILITY. USE AT YOUR OWN RISK
WARNING  : SHA1 of C:\nsrl_check\nsrl_check\check.exe : a1caf5d125e87cfc933529c
a64df127f82302ab7
```

Grid Subject Matter Experts, LLC  
1847 Iron Point Road, Suite 140, Folsom, CA 95630  
(916) 800-4534 | [www.gridsmc.com](http://www.gridsmc.com)  
[security@gridsmc.com](mailto:security@gridsmc.com)



5. The syntax is as follows: [Directory or File Path to Hash] [File path to Kaspersky\_RDS.zip]
  - a. Ex: to recursively hash the entire C: directory and compare against NSRL database (this may take a few minutes!):
  - b. Ex:

```
C:\Windows\system32>C:\nsrl_check\nsrl_check\check.exe C: C:\nsrl_check\nsrl_ckeck\Kaspersky_RDS.zip
```

6. If any Kaspersky product hashes are found, the output will look like the below, indicating you'll need to investigate further:

- a. Ex:

```
C:\Windows\system32>C:\nsrl_check\nsrl_check\check.exe "C:\Program Files (x86)"
C:\nsrl_check\nsrl_check\Kaspersky_RDS.zip
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus
18.0.0 matching ['FAF95EC65CDE5BD833CE610BB8523363310EC4AD', '4003E34416EBD25E4
C115D49DC15E1A7', 'B63FC1D8', 'dbghe lp.dll', '1213200', '182905', '358', ''] True
e
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus
18.0.0 matching ['29A33339B75DABE57BCD0A63DA49F969F968A843', 'EAF821D2AC2157609
6D597208462D31B', 'ABF6E58A', 'dbghe lp.prg', '706', '182905', '358', ''] True
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus
18.0.0 matching ['DA39A3EE5E6B4B0D325BF95601890AFD80709', 'D41D8CD98F00B204E
9800998ECF8427E', '00000000', 'wangbe.map', '0', '10971', '358', ''] True
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus
18.0.0 matching ['0CA477062FADD857B85703E6B2F51CA50B57B9C2', 'A63C1A26C69E3654F
BA3F288FC996587', 'F7A61BF5', 'kl.pbv', '214', '182905', '358', ''] True
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus
18.0.0 matching ['A23044FC0B3FFA3651C6622AEE5188C08942C443', '212D2D1D62D86325E
E6BAC1CDEA186F0', '4FF3FDC6', 'kl.ur1', '50', '182905', '358', ''] True
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus
18.0.0 matching ['646EB8784D020DA390BBCAD8BFD8DA28EC3C142F', '89B02032F92AC8330
47B834A203F591A', '52D387B5', 'oper.pbv_1', '239', '182905', '358', ''] True
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus
18.0.0 matching ['D58234A25C9DC416850B0FA2136681D757911C67', '5A0E82BFC43184707
7A49BC09D6357F0', 'BE42C95E', 'opera_banner_deny.vbs', '333', '16280', '358', '']
] True
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus
18.0.0\skin\resources\nneutral\locs matching ['DA39A3EE5E6B4B0D325BF95601890A
FD80709', 'D41D8CD98F00B204E9800998ECF8427E', '00000000', 'wangbe.map', '0', '10
971', '358', ''] True
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus
18.0.0\skin\resources\nneutral\sounds matching ['DAFB8F42C618D6EFA2DA8041F83F499
5C565A53B', 'DC74FE6687F9F19FEA175DA27295EE09', '78F2EDBD', 'skin_sounds_infecte
d.wav', '520712', '16280', '358', ''] True
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus
18.0.0\skin\resources\nneutral\sounds matching ['7E03E5B5616A6E652A754C6DF149B6A
45BBD572A', '839F5481A48F676831206734226007A1', 'CD098B8E', 'skin_sounds_infecte
d_p.wav', '79034', '16280', '358', ''] True
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Secure Conn
ection 2.0 matching ['FAF95EC65CDE5BD833CE610BB8523363310EC4AD', '4003E34416EBD
25E4C115D49DC15E1A7', 'B63FC1D8', 'dbghe lp.dll', '1213200', '182905', '358', '']
True
Detected: Found file C:\Program Files (x86)\Kaspersky Lab\Kaspersky Secure Conn
ection 2.0 matching ['29A33339B75DABE57BCD0A63DA49F969F968A843', 'EAF821D2AC215
76096D597208462D31B', 'ABF6E58A', 'dbghe lp.prg', '706', '182905', '358', ''] True
e
- Complete
```