Sigcheck - Sysinternals

By markruss

Archived: 2026-04-05 22:40:01 UTC

By Mark Russinovich

Published: February 4, 2026

 **Download Sigcheck (645 KB)**

Sigcheck is a command-line utility that shows file version number, timestamp information, and digital signature details, including certificate chains. It also includes an option to check a file's status on VirusTotal, a site that performs automated file scanning against over 40 antivirus engines, and an option to upload a file for scanning.

usage:

```
 sigcheck [-a][-h][-i][-e][-l][-n][[-s]|[-c|-ct]|[-m]][-q][-r][-u][-vt][-v[r][s]][-f catalog file] <file or dire

sigcheck -d [-c|-ct] <file or directory>

usage: sigcheck -t[u][v] [-i] [-c|-ct] <certificate store name|*>
```

Parameter	Description
-a	Show extended version information. The entropy measure reported is the bits per byte of information of the file's contents.
-accepteula	Silently accept the Sigcheck EULA (no interactive prompt)
-c	CSV output with comma delimiter
-ct	CSV output with tab delimiter
-d	Dump contents of a catalog file
-e	Scan executable images only (regardless of their extension)
-f	Look for signature in the specified catalog file
-h	Show file hashes
-i	Show catalog name and signing chain
-l	Traverse symbolic links and directory junctions

Parameter	Description
-m	Dump manifest
-n	Only show file version number
-o	Performs Virus Total lookups of hashes captured in a CSV file previously captured by Sigcheck when using the -h option. This usage is intended for scans of offline systems.
-nobanner	Do not display the startup banner and copyright message.
-r	Disable check for certificate revocation
-p	Verify signatures against the specified policy, represented by its GUID.
-s	Recurse subdirectories
-t[u][v]	Dump contents of specified certificate store ('*' for all stores). Specify -tu to query the user store (machine store is the default). Append '-v' to have Sigcheck download the trusted Microsoft root certificate list and only output valid certificates not rooted to a certificate on that list. If the site is not accessible, authrootstl.cab or authroot.stl in the current directory are used instead, if present.
-u	If VirusTotal check is enabled, show files that are unknown by VirusTotal or have non-zero detection, otherwise show only unsigned files.
-v[rs]	Query VirusTotal (www.virustotal.com) for malware based on file hash. Add 'r' to open reports for files with non-zero detection. Files reported as not previously scanned will be uploaded to VirusTotal if the 's' option is specified. Note scan results may not be available for five or more minutes.
-vt	Before using VirusTotal features, you must accept VirusTotal terms of service. See: https://www.virustotal.com/en/about/terms-of-service/ If you haven't accepted the terms and you omit this option, you will be interactively prompted.

One way to use the tool is to check for unsigned files in your `\Windows\System32` directories with this command:

```
sigcheck -u -e c:\windows\system32
```

You should investigate the purpose of any files that are not signed.

 **Download Sigcheck (645 KB)**

Runs on:

- Client: Windows 8.1 and higher
- Server: Windows Server 2012 and higher

- Nano Server: 2016 and higher
- Malware Hunting with the Sysinternals Tools
  In this presentation, Mark shows how to use the Sysinternals tools to identify, analyze and clean malware.
