Checksum

Return to Glossary

A **Checksum** is a value that represents the number of bits in a transmission message and is used by IT professionals to detect high-level errors within data transmissions. Prior to transmission, every piece of data or file can be assigned a **Checksum** value after running a cryptographic hash function. The term **Checksum** is also sometimes seen as hash sum or hash value.

Checksums work by giving the party on the receiving end information about the transmission to make sure that the full range of data is fully delivered. The **Checksum** value itself is typically a long string of letters and numbers that act as a sort of fingerprint for a file or set of files to indicate the number of bits included in the transmission.

If the **Checksum** value calculated by the end user is even slightly different from the original **Checksum** value of the file, it can alert all parties in the transmission that the file was corrupted or tampered with by a third party. From there, the receiver can investigate what went wrong or try re-downloading the file.

The common protocols used to determine **Checksum** numbers are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). TCP is typically more reliable for tracking transmitted packets of data, but UDP may be beneficial to avoid slowing down transmission time.

Source: https://www.techtarget.com/searchsecurity/definition/checksum