

Fingerprints

What are digital fingerprints and why are they useful?

By IP.com

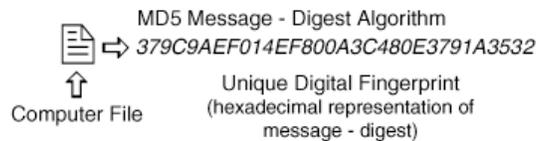


Introduction

Digital fingerprint methodology lies in the field of mathematics called cryptography.

A digital fingerprint is a unique digital representation of a single computer file or piece of digital data. The methodology enables a computer file to be encrypted such that it is computationally infeasible to obtain the same fingerprint from two different files. Furthermore, there is no way to recreate all or any part of the original file from the fingerprint. Hence, the human fingerprint analogy is appropriate: each person has a unique fingerprint, and it is not possible to determine a person's identity from a fingerprint, unless one has previously generated a list that correlates specific people with specific fingerprints. In other words, like your own fingerprint, your file's fingerprint is unique.

The fingerprinting methodologies used by IP.com are based on the public domain [MD5 Message-Digest Algorithm](#) (RFC 1321), and SHA-1 [Secure Hashing Algorithm](#) (RFC 3174), which are one-way, hash (or message digest) functions. The message-digest that is created when the algorithm is applied to a file consists of a unique string of 128 bits (for MD5), 160 bits (for SHA-1), or 288 bits (for combination MD5/SHA-1). The fingerprints utilized by IP.com are hexadecimal representations of these message-digests. In some cases, a Base64 encoded version of the fingerprint is used in order to reduce the character count necessary to reproduce the fingerprint in print. IP.com uses [standard Base64 character-encoding techniques](#), such as those used by Internet email and newsreaders. The following diagram illustrates this process and shows an example of a digital fingerprint created using the MD5 Message-Digest Algorithm:



Integrity of File Transmission

Digital fingerprints are very useful for verifying the integrity of file transmissions. Many file transfer protocols take advantage of this capability for automatic error detection. In such a process, the fingerprint of a file is transmitted along with the file itself. Upon receipt of the transmission, the recipient computer generates a fingerprint of the file, as received. If the transmitted fingerprint does not match the fingerprint of the received file, then the system knows that a transmission error has occurred.

Be Sure to Check Your Fingerprints

We supply a simple utility called HashValue that you can run on your Microsoft Windows computer to generate fingerprints from your files. This utility, packaged from IP.com, returns MD5 and SHA-1 fingerprints for the file specified. It is based on public domain implementations of the MD5 Message-Digest Algorithm and SHA-1 Secure Hashing Algorithm.

After publication at IP.com, you will receive an email notification, which contains fingerprints for your primary document and attachment(s), as received by and published at IP.com. It is recommended that you create fingerprints of your original files and compare these to the fingerprints in the email. When the fingerprints match, you have assurance that your document was published in its original form, without error. In the event that your document is later involved in litigation, this assurance could be critical.

Document Authentication

At any time in the future, a fingerprint can be made from your document on file in the IP.com database, and the resulting fingerprint compared to the fingerprint that was generated during publication of your document at IP.com. If the two fingerprints are identical, then you have proof that the content of your document was not altered by anyone after publication. Your fingerprints, along with a timestamp, are included in the digital notarization during the IP.com publication process.

This combination of digital fingerprinting and notarization provides a foolproof way to verify publication date and authenticity.

Comparison with the Conventional Process

It is interesting to compare this digital process to the conventional process, where a document can be printed out or rewritten with any date on it, or with any of the content altered. For example, using a word processor, a document can be printed out multiple times on the same day, with several different dates on it. Or it can be printed out many times on different dates, with the same date on each printout. Notarization can help with this process, but even it has limitations in the case of conventional documents. Here's why. Let's say you print out a 10-page document, and you sign and have it notarized on the last page (page 10). In theory, there is no reason you cannot later go back and change something on pages 1-9, and attach the notarized page 10 to the altered document.

With IP.com's digital fingerprinting and notarization process, this isn't possible, since the notarization includes the file's fingerprint.