

ssdeep - Latest version 2.7

Quick Links

- [Download ssdeep](#)
- [The ssdeep man page](#)
- [Changelog](#)
- [Quickstart Guide](#)
- [API documentation](#)
- [Sourceforge project page](#) - Home to ssdeep development and feature requests

Introduction

ssdeep is a program for computing context triggered piecewise hashes (CTPH). Also called fuzzy hashes, CTPH can match inputs that have homologies. Such inputs have sequences of identical bytes in the same order, although bytes in between these sequences may be different in both content and length.

A complete explanation of CTPH can be found in [*Identifying almost identical files using context triggered piecewise hashing*](#) from the journal Digital Investigation. There is a free version of this paper available through the Digital Forensic Research Workshop conference, [free version of *Identifying almost identical files using context triggered piecewise hashing*](#).

There are some usage scenarios in the [Quickstart guide](#) and the [Forensics Wiki entry on ssdeep](#).

The package also includes a fuzzy hashing API. The API is documented in the file API.TXT in the Windows distribution and README in the source code package.

See Also

The math behind fuzzy hashing was originally developed by Dr. Andrew Triggall in a spam detector he called [spamsum](#).

Supported Platforms

Microsoft Windows

The program runs on Microsoft Windows 2000, XP, 2003, and Vista. It is *not* supported on Windows 95, 98, Me, 3.1, 3.11, or 3.11 for Workgroups.

*nix

The program has been tested on Open Solaris, FreeBSD, Linux, and Mac OS X. It should compile and run on any other platform that is supported by the GNU Build Tools.

Download

Stable Version

The latest stable version of ssdeep is version 2.7 and was released on 30 Sep 2011. You can take a look at the [complete changelog](#), but here are the changes in the latest version:

- Added ability to process standard input, up to 100MB
- Added a warning message when the program does not have enough input to make a meaningful result

Version 2.7	30 Sep 2011	Windows binary	SHA256 da483426a1c887a5a425f689cb22c9040fb668559e6f0c3604237d820bb3b57b
		source code	SHA256 b76a60a8f96789895703316ed3b36d1f0c1f35be892d875b69b0a1f814472a36

Beta Version

There is no beta version of ssdeep right now. If you have any problems or would like to see something added to ssdeep, please send mail to the developer at [research at\) jessekornblum !dot\) com](mailto:research@jessekornblum.com) or visit the [Sourceforge project page](#).

Older Versions

Although older versions of ssdeep are available for historical purposes, you shouldn't use these unless you have a truly compelling reason.

[Show older versions](#)

License

The ssdeep program and its API are licensed under the terms of version 2 of [the GNU General Public License](#).

About the developer

ssdeep was written by Jesse Kornblum of the [ManTech International Corporation](#). Please send all

correspondence to research *at jessekornblum .dot com.

Acknowledgements

Code for the threshold mode contributed by Jason Sherman. The testing of this program was made possible in part thanks to the generosity of the Computer Science Department at the University of Iowa.

This page was last updated on 18 Jan 2012.

