Emulator - Emulator Issues #11520

Add better hashing algorithms for checking disc images

01/07/2019 02:38 AM - Jebeld17@gmail.com

Status:	Accepted	**% Done:**	0%
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Operating system:	N/A	**Relates to performance:**	No
Issue type:	Feature request	**Easy:**	No
Milestone:		**Relates to maintainability:**	No
Regression:	No	**Regression start:**	
Relates to usability:	No	**Fixed in:**	

Description

MD5Sums are the preferred way (and only way) included in Dolphin to check the integrity of my game files, but MD5 has known flaws, downsides, and vulnerabilities.

With these problems MD5 has, newer methods of file hashing have been replacing MD5 in most programs - such as MD256, MD512, and higher. It's time Dolphin gains official support and the in-app tools to support these more complex algorithms, too, and help push MD5 to the past.

History

#1 - 01/07/2019 02:40 AM - Jebeld17@gmail.com

*SHA256

#2 - 01/07/2019 07:52 AM - JosJuice

- Issue type changed from Bug to Feature request

- Status changed from New to Accepted

- Subject changed from Replace MD5SUM with ≥MD256SUMs to Add better hashing algorithms for checking disc images

We won't remove the option to calculate MD5, since it (along with SHA1) is commonly used in lists of hashes that you can find online. Adding the ability to also calculate SHA256 makes sense, though.

#3 - 01/07/2019 05:22 PM - Jebeld17@gmail.com

Thank you :-)
With this said, ≥ SHA256 should definitely be the default choice for Dolphin and warnings should be in-place for users stating the implications of MD5.

JosJuice wrote:

> We won't remove the option to calculate MD5, since it (along with SHA1) is commonly used in lists of hashes that you can find online. Adding the ability to also calculate SHA256 makes sense, though.

#4 - 01/07/2019 05:26 PM - BhaaL

Those hashes are used for integrity, not security, so they do not really matter that much.
As already mentioned, the goal is to provide some sort of comparison value (to verify whether a dump is good or not) against well-known public lists (such as GameTDB amongst others).

#5 - 01/08/2019 12:20 PM - Billiard26

Is there even a database of GC/Wii game non-md5 checksums to compare to..?

#6 - 01/08/2019 12:21 PM - JosJuice

Redump uses CRC32/MD5/SHA1, and GameTDB does the same. I don't think there is any database that is using SHA256, really...

#7 - 01/08/2019 12:23 PM - Billiard26

I'm only seeing md5 on GameTDB. At least for the few (very popular) games that I looked at. MD5 definitely seems to be the most popular and it does the job (of testing integrity) just fine.

#8 - 01/08/2019 12:29 PM - Armada

The only possible security issue I can see is if someone were to make malware for Dolphin and then manages to make its hash collide with a legitimate game for extra points.

I doubt anyone would go through that much trouble, because no one would check the MD5 anyway before running the ISO.

#9 - 01/08/2019 12:31 PM - JosJuice

Not all games have all types of hashes on GameTDB, but those are the three types of hashes that the GameTDB database supports. https://www.gametdb.com/Wii/RSBE01 is an example of a game that has all three types.