

# Forum:[Hack Forums](#)

Thread: [\[TUT\] Identifying Hashes](#)

**Legion.** - January 18, 2015, 11:36 am

This is how to identify different types of hashes.

MD5

They are always 32 characters in length (128 Bits)

They are always hexadecimal (Only characters 0-9 and A-F)

Sha1

They are always 40 Characters in length (160 bits)

They are always hexadecimal (Only characters 0-9 and A-F)

MySQL < 4.1

They are always 16 Characters in length (64 bits)

They are always hexadecimal (Only characters 0-9 and A-F)

NOTE: These are not used very often.

MYSQL5

They are always 41 characters in length

They are always capitalized

They always begin with an asterisk

MD5(Wordpress) These are used in Wordpress Sites

They always start with \$P\$

They are always variable case alpha numeric (0-9 A-Z a-z)

They are always 34 characters long

MD5/phpBB3) Used in PHPBB Forums

They always start with \$H\$

They are always variable case alpha numeric (0-9 A-Z a-z)

They are always 34 characters long

Remember to check for salts! That's it for now, bye bye!

Helpdesk: <https://hackforums.net/showthread.php?tid=4642939>

**chick3nman** - January 18, 2015, 12:03 pm

(Jan 18, 2015 12:36 PM)Legion. Wrote: [\[CITE\]](#) -snip-

I hate the be that guy but some of this is wrong or only partially right. For one, MySQL 5 hashes do start with an asterisk upon generation, but a lot of times that asterisk is stripped off before the hash is passed around or cracked (programs like hashcat do not accept the asterisk when loading). Generally the only way you can tell a MySQL 4.1/5 hash from any other 40 character hash (like SHA-1) is that they are stored in all uppercase so unless someone has toggled case on a 40 character hash, it can be somewhat safe to assume its MySQL 4.1/5 if it's all uppercase.

Also for the MD5(Wordpress), MD5/phpBB3) hashes, they are encoded upon generation so the output actually includes Upper, Lower, Digits(numbers), and symbols (specifically periods "." and forward slashes "/"), not just alpha numeric.

And lastly, only two of the hash types you listed can have separated salts, MD5 and SHA-1. MySQL(all versions) are not salted(to my knowledge). PHPass(Wordpress/phpBB3) have the salt included right after the round number in the hash. The beginning of the hash is the identifier(\$H\$ or \$P\$), then the round number comes after the second \$(usually 9 but it's not decimal so the 9 really represents 11 rounds), then the next 8 characters are the salt. The remainder is the actual hashed password.

**Xorex** - January 18, 2015, 12:33 pm

MyBB - 8 Character Salt

IPB - 5 Character Salt

vBulletin (Old) - 3 Character Salt

vBulletin (New) - 30 Character Salt

**shawnw1104** - January 18, 2015, 12:45 pm

well there are simpler ways to do this that does not involve any manual work :P

there are tools out there that can do all the work for you,

<https://hackforums.net/showthread.php?tid=4642896>

or if you want a website then,

<http://www.dfcode.org/onlinehashidentifier.php>

...

Shawn W.

**?Saint** - January 18, 2015, 1:15 pm

Best way to identify a hash is to just look here.

[http://hashcat.net/wiki/doku.php?id=example\\_hashes](http://hashcat.net/wiki/doku.php?id=example_hashes)

**chick3nman** - January 18, 2015, 1:16 pm

(Jan 18, 2015 02:15 PM)?Saint Wrote: [\[CITE\]](#) Best way to identify a hash is to just look here.

[http://hashcat.net/wiki/doku.php?id=example\\_hashes](http://hashcat.net/wiki/doku.php?id=example_hashes)

Yup, That's one of the most visited pages on my browser :P

EDIT: Checked my visit stats, seems it's no where near as many times as i visited the cryptography section in here. I may need to go outside for a while after seeing those numbers.

**Legion.** - January 18, 2015, 1:26 pm

(Jan 18, 2015 02:16 PM)chick3nman Wrote: [\[CITE\]](#) Yup, That's one of the most visited pages on my browser :P

EDIT: Checked my visit stats, seems it's no where near as many times as i visited the cryptography section in here. I may need to go outside for a while after seeing those numbers.Oh, lol. Wrote tutorial for nothing. ? ?