

# Forum:[Hack Forums](#)

Thread: [Identifying Hashes / Encryption Help](#)

**M?tt** - September 7, 2024, 7:43 am

So I'm trying to figure out some good resources to compile regarding identifying hashes and encryptions. I know that sometimes Hashcat and CyberChef can identify the algorithm, but what about hashes sent through multiple iterations or even multiple and different algorithms.

I know there's a few knowledgeable members on here and I'm hoping I can get some guidance in the right direction.

**Bastille** - September 7, 2024, 7:51 am

I'm veeeeery interested in this topic, would you mind to share the resources once they have been compiled ?

The following is simple but, couldn't we ask ChatGPT in such cases ? Did you try already ? Do you have examples of hashes ?

**M?tt** - September 7, 2024, 7:53 am

(Sep 7, 2024 07:51 AM)Bastille Wrote: [\[CITE\]](#) I'm veeeeery interested in this topic, would you mind to share the resources once they have been compiled ?

The following is simple but, couldn't we ask ChatGPT in such cases ? Did you try already ? Do you have examples of hashes ?

I didn't think to ask ChatGPT; probably a habit I should start doing honestly.

I don't have hashes exactly as an example (yet). It's more for a CTF that I'm preparing for and this is one of my weaker areas. I'd like to improve to give my team a better chance at winning and also it'll be great to understand and maybe help out here more.

I know ultimately having a machine to run the cracking is great, but I'm just operating out of a VM right now. I haven't invested in a VPS or something to do any cracking since it's not my focus area right now.

**DramaKing** - September 7, 2024, 8:09 am

Hashes.com is my go-to. There are likely proprietary hashes from surveillance software that I haven't been able to successfully identify, but the site otherwise is able to give best effort results.

**M?tt** - September 7, 2024, 8:11 am

(Sep 7, 2024 08:09 AM)DramaKing Wrote: [\[CITE\]](#) Hashes.com is my go-to. There are likely proprietary hashes from surveillance software that I haven't been able to successfully identify, but the site otherwise is able to give best effort results.

I've used Hashes.com as well, but I've had instances when it doesn't return anything back. I can't remember which video it was, but I recall IppSec going over in a HTB CTF about what certain hashes look like or contain. That's really where I'm trying to posture this conversation.

Actually just threw my question into ChatGPT and got some good information from that. I really need to use ChatGPT more.

But if there's any writeups or useful tools, I'll take that as well.

**DramaKing** - September 7, 2024, 8:15 am

(Sep 7, 2024 08:11 AM)M?tt Wrote: [\[CITE\]](#) I've used Hashes.com as well, but I've had instances when it doesn't return anything back. I can't remember which video it was, but I recall IppSec going over in a HTB CTF about what certain hashes look like or contain. That's really where I'm trying to posture this conversation.

Well, due to the nature of hashes, if you identify a hash that has gone through multiple algorithms, you wouldn't be able to identify the series of operations.

**M?tt** - September 7, 2024, 8:24 am

(Sep 7, 2024 08:15 AM)DramaKing Wrote: [\[CITE\]](#) Well, due to the nature of hashes, if you identify a hash that has gone through multiple algorithms, you wouldn't be able to identify the series of operations.

That's kind of where I'm trying to posture this thread towards. Identifying the first hash and then finding a match could lead to another hash. I'm just wondering what tactics can be used to determine the "right" direction. Seems like there isn't anything, but I'm curious how I can use metadata or information about the plaintext to help.

**DramaKing** - September 7, 2024, 9:01 am

(Sep 7, 2024 08:24 AM)M?tt Wrote: [\[CITE\]](#) That's kind of where I'm trying to posture this thread towards. Identifying the first hash and then finding a match could lead to another hash. I'm just wondering what tactics can be used to determine the "right" direction. Seems like there isn't anything, but I'm curious how I can use metadata or information about the plaintext to help.

And how do you expect to match a hash to another hash? Getting the source is the only feasible method, unless you can say "Oh, 0e1484eb061b8e9cfd81868bba1dc4a0:229381927:182719643 has a length that matches (md5(\$salt1.strtoupper(md5(\$salt2.\$pass)))) \* (hash mode 3730)."

**M?tt** - September 10, 2024, 4:56 pm

(Sep 7, 2024 09:01 AM)DramaKing Wrote: [\[CITE\]](#) And how do you expect to match a hash to another hash? Getting the source is the only feasible method, unless you can say "Oh, 0e1484eb061b8e9cfd81868bba1dc4a0:229381927:182719643 has a length that matches (md5(\$salt1.strtoupper(md5(\$salt2.\$pass)))) \* (hash mode 3730)."

Here's an example:

```
Stuff --MD5--> 9de26c5a027aa7e15c7f85fdfae4e785 --SHA1 (80 rounds)-->
9199df8df601e4ef057c4cc7597f1c9afe7f0551
```

So throwing the final result in there tells me it's SHA1 (from hashes.com), but I'm curious if there's ways (other than OSINT) to determine how to find the next step; which is obviously MD5. Multiple rounds definitely complicates things, but I'm curious if there's ways to identify this.

I hope this doesn't make me sound stupid, but that's why I'm asking (because I am stupid ?).