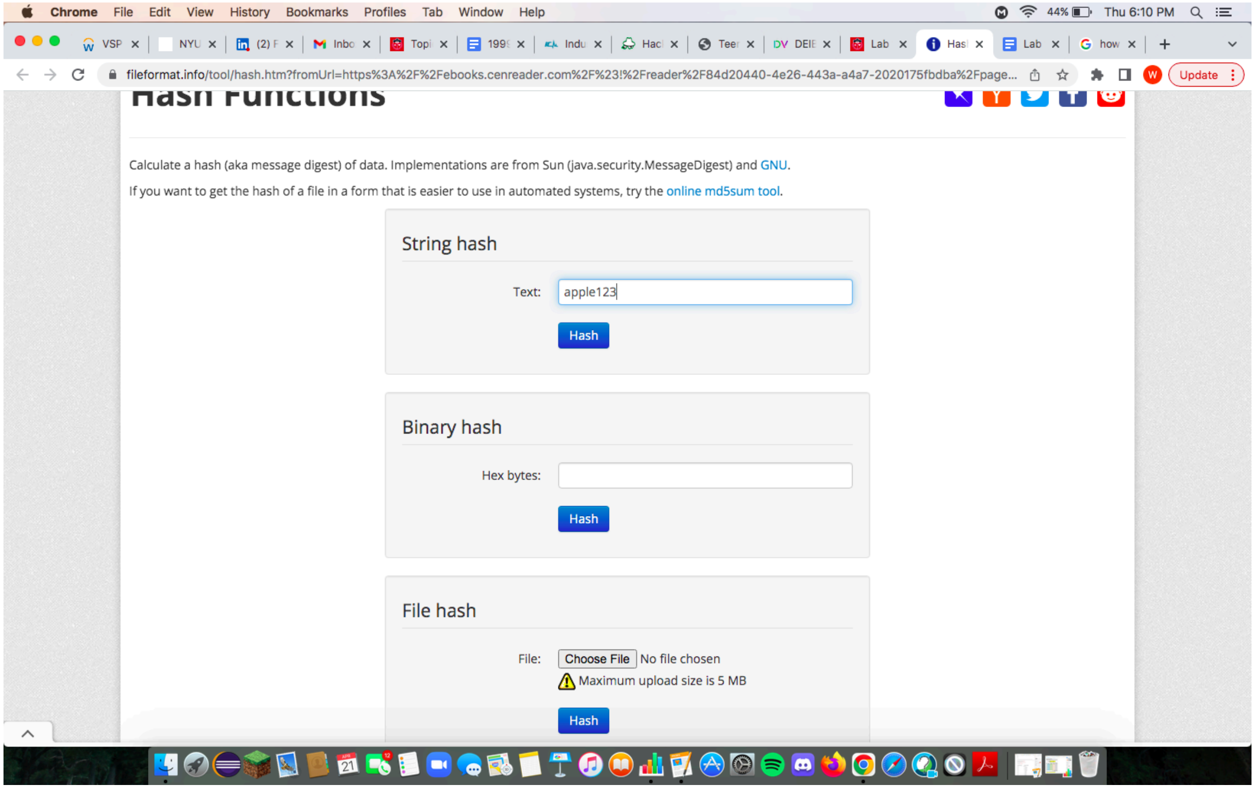
Project 12-1: Using an Online Password Cracker

1. The first step was to go to www.fileformat.info/tool/hash.htm and enter the password “apple123” in the string hash text box and then click the hash button.


Chrome File Edit View History Bookmarks Profiles Tab Window Help
44% Thu 6:10 PM
fileformat.info/tool/hash.htm?fromUrl=https%3A%2F%2Febooks.cenreader.com%2F%23!%2Freader%2F84d20440-4e26-443a-a4a7-2020175fbdba%2Fpage...
Update
Hash Functions

Calculate a hash (aka message digest) of data. Implementations are from Sun (java.security.MessageDigest) and GNU.

If you want to get the hash of a file in a form that is easier to use in automated systems, try the online md5sum tool.

String hash

Text: apple123

Hash

Binary hash

Hex bytes:

Hash

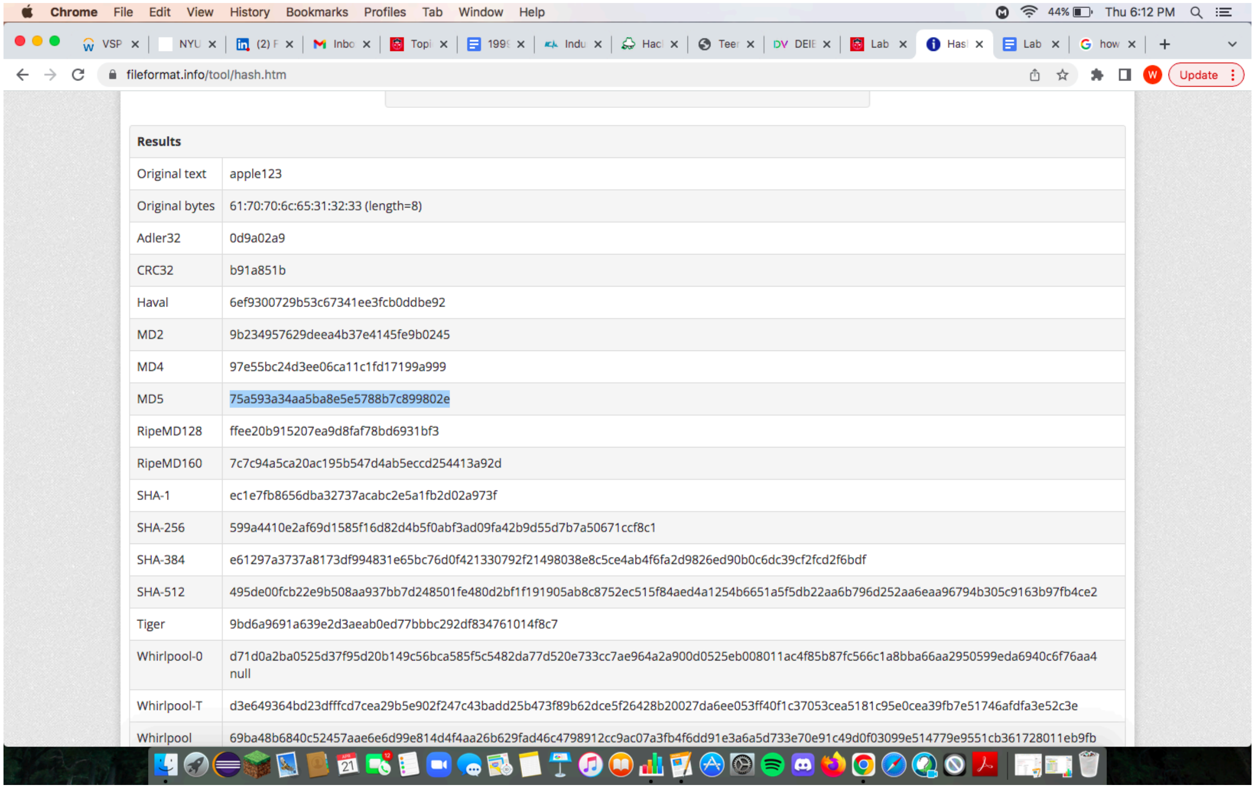
File hash

File: Choose File No file chosen

⚠ Maximum upload size is 5 MB

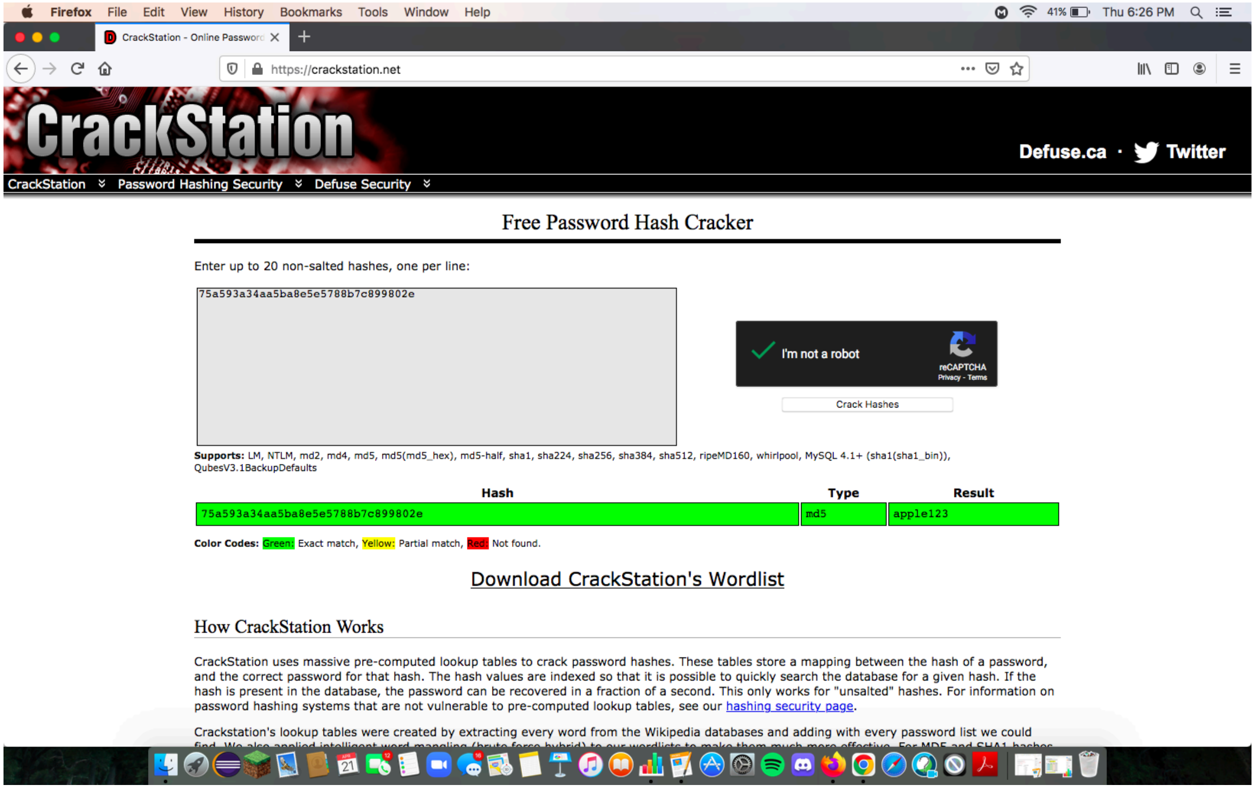
Hash

2. The next step is to scroll down to the list of different hashes and look at the hash named “MD5”. The MD5 hash for “apple123” is 75a593a34aa5ba8e5e5788b7c899802e. We need to copy this hash and then go to the website called https://crackstation.net/.


Chrome File Edit View History Bookmarks Profiles Tab Window Help
44% Thu 6:12 PM
fileformat.info/tool/hash.htm
Update

Results	
Original text	apple123
Original bytes	61:70:70:6c:65:31:32:33 (length=8)
Adler32	0d9a02a9
CRC32	b91a851b
Haval	6ef9300729b53c67341ee3fcb0ddbe92
MD2	9b234957629deea4b37e4145fe9b0245
MD4	97e55bc24d3ee06ca11c1fd17199a999
MD5	75a593a34aa5ba8e5e5788b7c899802e
RipeMD128	ffee20b915207ea9d8faf78bd6931bf3
RipeMD160	7c7c94a5ca20ac195b547d4ab5eccd254413a92d
SHA-1	ec1e7fb8656dba32737acabc2e5a1fb2d02a973f
SHA-256	599a4410e2af69d1585f16d82d4b5f0abf3ad09fa42b9d55d7b7a50671ccf8c1
SHA-384	e61297a3737a8173df994831e65bc76d0f421330792f21498038e8c5ce4ab4f6fa2d9826ed90b0c6dc39cf2fcd2f6bdf
SHA-512	495de00fcb22e9b508aa937bb7d248501fe480d2bf1f191905ab8c8752ec515f84aed4a1254b6651a5f5db22aa6b796d252aa6eaa96794b305c9163b97fb4ce2
Tiger	9bd6a9691a639e2d3aeab0ed77bbbc292df834761014f8c7
Whirlpool-0	d71d0a2ba0525d37f95d20b149c56bca585f5c5482da77d520e733cc7ae964a2a900d0525eb008011ac4f85b87fc566c1a8bba66aa2950599eda6940c6f76aa4 null
Whirlpool-T	d3e649364bd23dfffcd7cea29b5e902f247c43badd25b473f89b62dce5f26428b20027da6ee053ff40f1c37053cea5181c95e0cea39fb7e51746afdfa3e52c3e
Whirlpool	69ba48b6840c52457aae6e6d99e814d4f4aa26b629fad46c4798912cc9ac07a3fb4f6dd91e3a6a5d733e70e91c49d0f03099e514779e9551cb361728011eb9fb

3. The next step is to paste the MD5 hash into the box that allows for 20 unsalted hashes. After pasting it into the box, click the box named “crack hashes.” The website cracked the hash almost instantly.



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
75a593a34aa5ba8e5e5788b7c899802e
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
75a593a34aa5ba8e5e5788b7c899802e	md5	apple123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

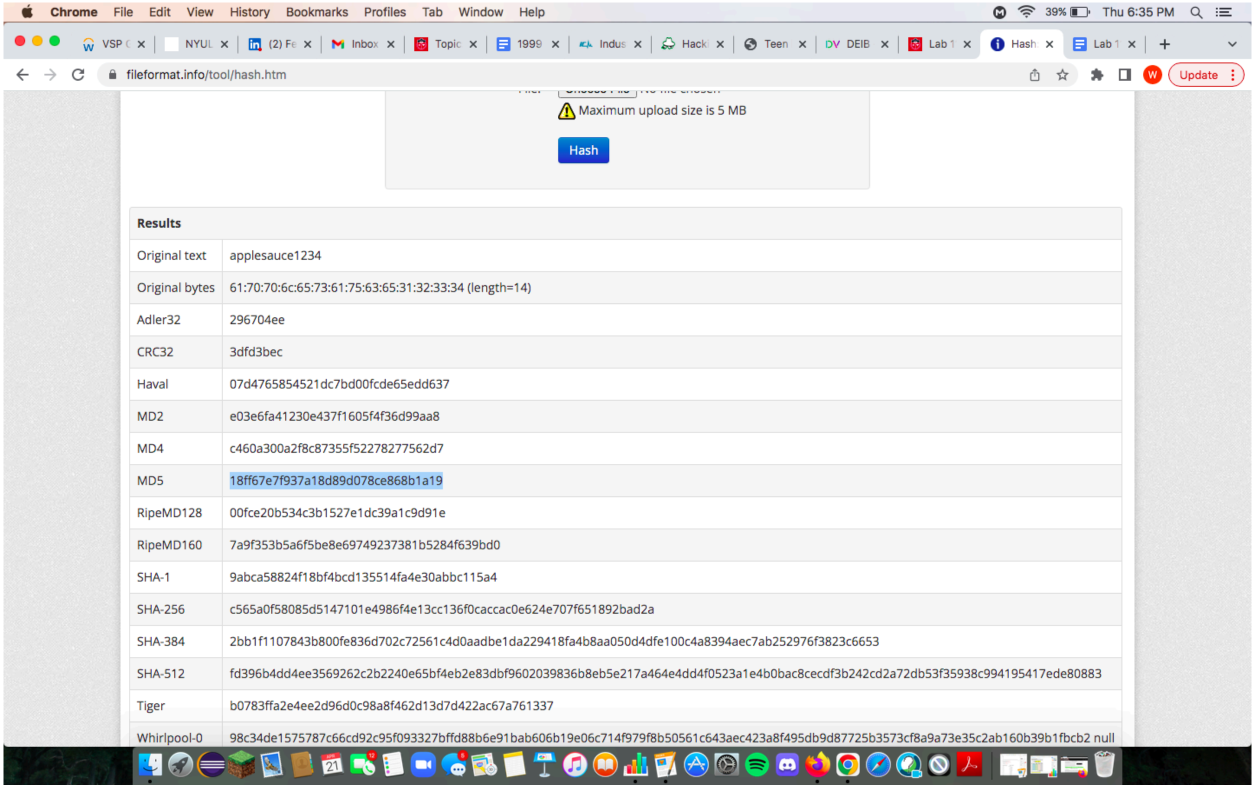
Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

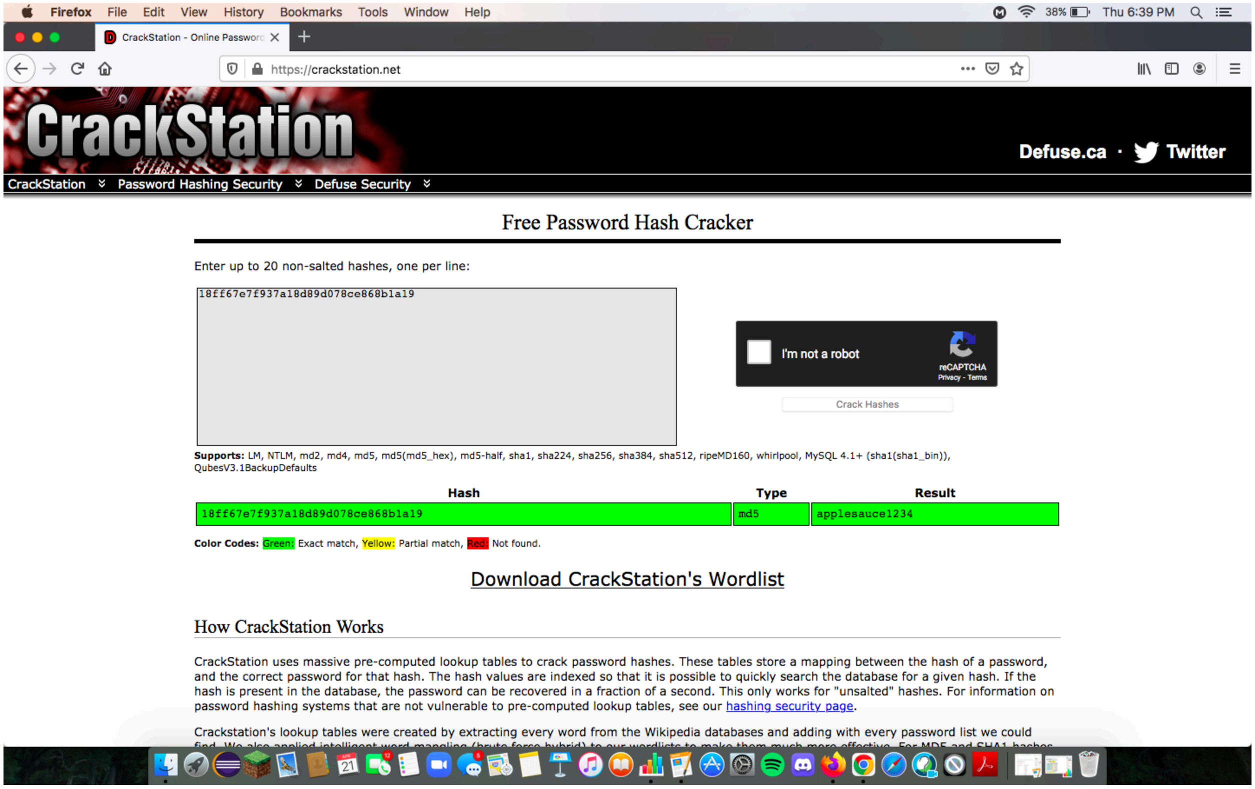
Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes

4. The next step is to return to the original website and enter this password “applesauce1234” in the textbox, click hash, and then copy the MD5 hash again.



Results	
Original text	applesauce1234
Original bytes	61:70:70:6c:65:73:61:75:63:65:31:32:33:34 (length=14)
Adler32	296704ee
CRC32	3dfd3bec
Haval	07d4765854521dc7bd00fcde65edd637
MD2	e03e6fa41230e437f1605f4f36d99aa8
MD4	c460a300a2f8c87355f52278277562d7
MD5	18ff67e7f937a18d89d078ce868b1a19
RipeMD128	00fce20b534c3b1527e1dc39a1c9d91e
RipeMD160	7a9f353b5a6f5be8e69749237381b5284f639bd0
SHA-1	9abca58824f18bf4bcd135514fa4e30abbc115a4
SHA-256	c565a0f58085d5147101e4986f4e13cc136f0caccac0e624e707f651892bad2a
SHA-384	2bb1f1107843b800fe836d702c72561c4d0aadbe1da229418fa4b8aa050d4dfe100c4a8394aec7ab252976f3823c6653
SHA-512	fd396b4dd4ee3569262c2b2240e65bf4eb2e83dbf9602039836b8eb5e217a464e4dd4f0523a1e4b0bac8cecdf3b242cd2a72db53f35938c994195417ede80883
Tiger	b0783ffa2e4ee2d96d0c98a8f462d13d7d422ac67a761337
Whirlpool-0	98c34de1575787c66cd92c95f093327bffd88b6e91bab606b19e06c714f979f8b50561c643aec423a8f495db9d87725b3573cf8a9a73e35c2ab160b39b1fbcb2 null

5. After copying the MD5 of the password, we go to the second website we visited earlier, and enter the hash into the website. It also took almost instantly to crack this hash


Firefox File Edit View History Bookmarks Tools Window Help
38% Thu 6:39 PM
CrackStation - Online Password
https://crackstation.net
CrackStation
Defuse.ca · Twitter
CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
18ff67e7f937a18d89d078ce868b1a19
```

I'm not a robot
reCAPTCHA
Privacy - Terms
Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
18ff67e7f937a18d89d078ce868b1a19	md5	applesauce1234

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

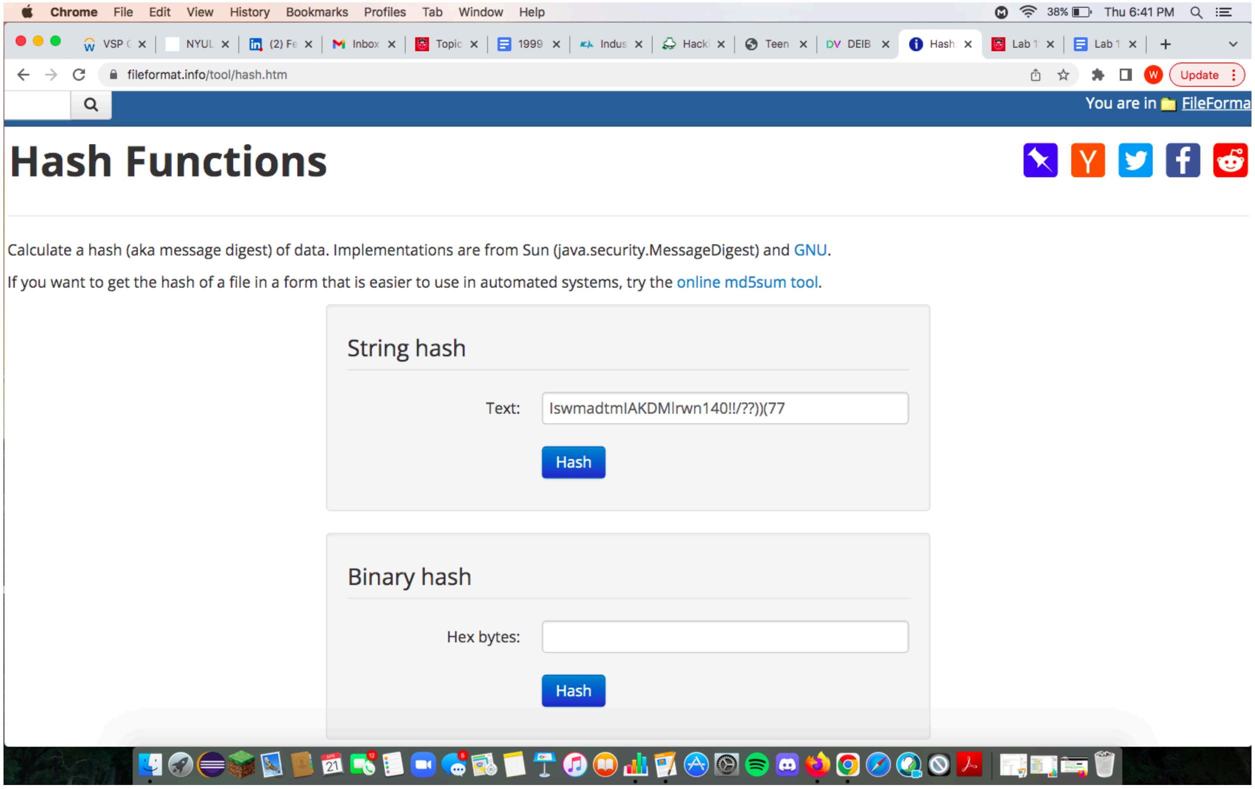
Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could

6. After doing that, I am going to revisit the first website that I viewed and enter a random password of my choosing and see how long that it takes for the password cracker to crack it.


Chrome File Edit View History Bookmarks Profiles Tab Window Help
38% Thu 6:41 PM
VSP NYUL (2) Fe Inbox Topic 1999 Indus Hack Teen DEIB Hash Lab 1 Lab 1
fileformat.info/tool/hash.htm
Update
You are in FileForma

Hash Functions

Calculate a hash (aka message digest) of data. Implementations are from Sun (java.security.MessageDigest) and GNU.

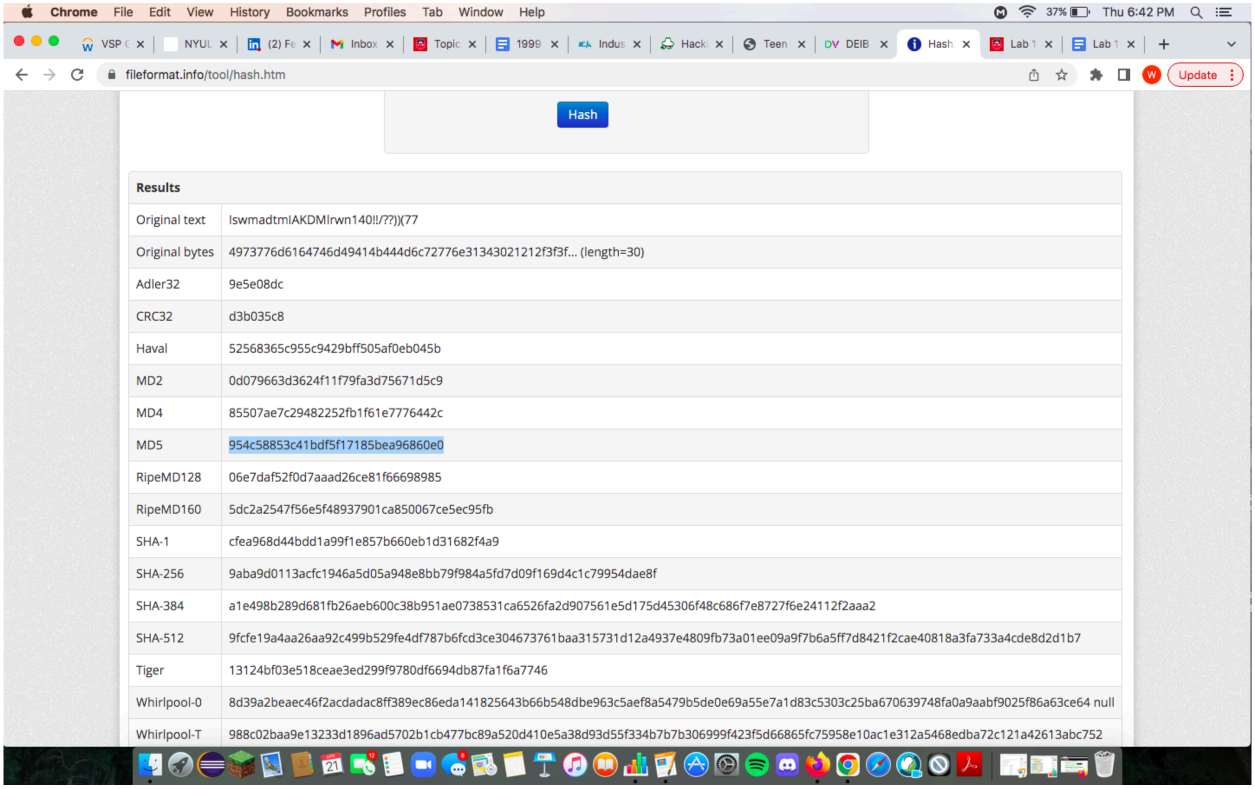
If you want to get the hash of a file in a form that is easier to use in automated systems, try the online md5sum tool.

String hash

Text: IswmadtmlAKDMlrwn140!!/??))(77

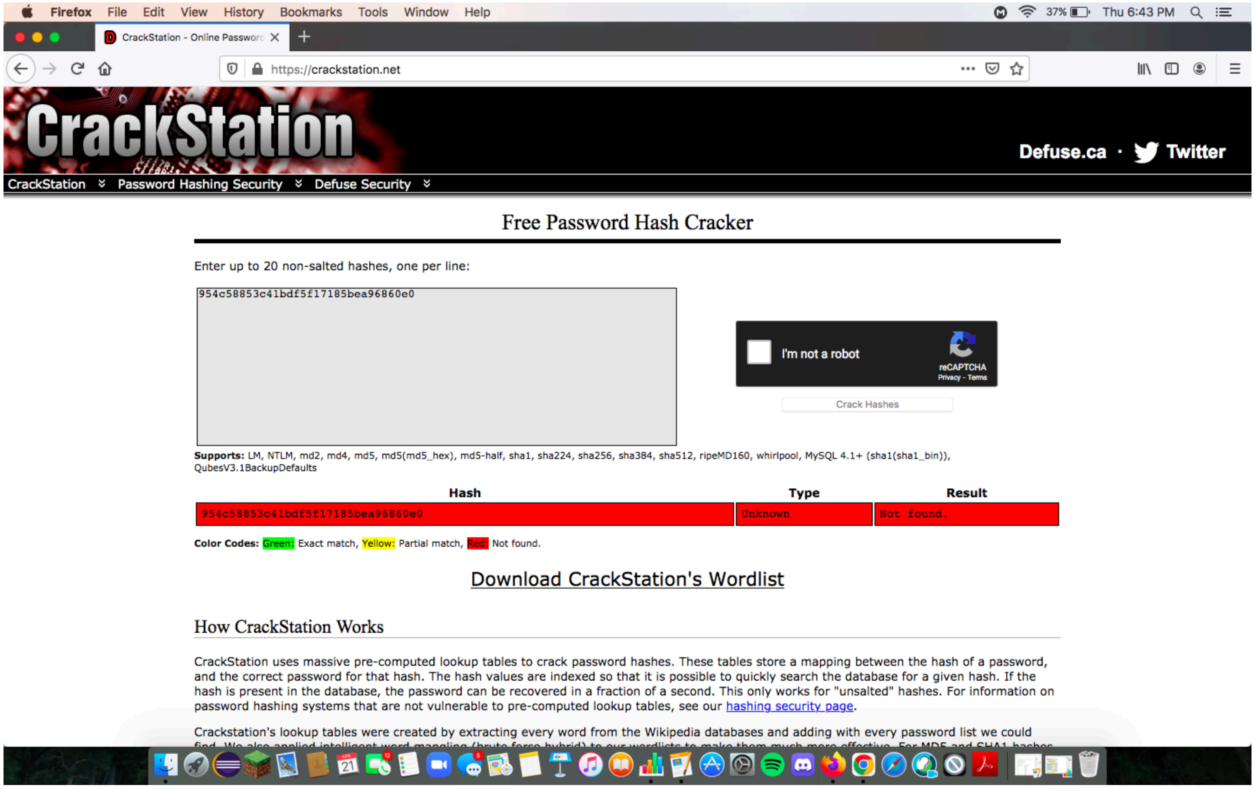
Binary hash

Hex bytes:



fileformat.info/tool/hash.htm

Results	
Original text	IswmadtmIAKDMIrwn140!!/??))(77
Original bytes	4973776d6164746d49414b444d6c72776e31343021212f3f3f... (length=30)
Adler32	9e5e08dc
CRC32	d3b035c8
Haval	52568365c955c9429bff505af0eb045b
MD2	0d079663d3624f11f79fa3d75671d5c9
MD4	85507ae7c29482252fb1f61e7776442c
MD5	954c58853c41bdf5f17185bea96860e0
RipeMD128	06e7daf52f0d7aaad26ce81f66698985
RipeMD160	5dc2a2547f56e5f48937901ca850067ce5ec95fb
SHA-1	cfea968d44bdd1a99f1e857b660eb1d31682f4a9
SHA-256	9aba9d0113acfc1946a5d05a948e8bb79f984a5fd7d09f169d4c1c79954dae8f
SHA-384	a1e498b289d681fb26aeb600c38b951ae0738531ca6526fa2d907561e5d175d45306f48c686f7e8727f6e24112f2aaa2
SHA-512	9fcfe19a4aa26aa92c499b529fe4df787b6fcd3ce304673761baa315731d12a4937e4809fb73a01ee09a9f7b6a5ff7d8421f2cae40818a3fa733a4cde8d2d1b7
Tiger	13124bf03e518ceae3ed299f9780df6694db87fa1f6a7746
Whirlpool-0	8d39a2beaec46f2acdadac8ff389ec86eda141825643b66b548dbe963c5aef8a5479b5de0e69a55e7a1d83c5303c25ba670639748fa0a9aabf9025f86a63ce64 null
Whirlpool-T	988c02baa9e13233d1896ad5702b1cb477bc89a520d410e5a38d93d55f334b7b7b306999f423f5d66865fc75958e10ac1e312a5468edba72c121a42613abc752



https://crackstation.net

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

954c58853c41bdf5f17185bea96860e0

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
954c58853c41bdf5f17185bea96860e0	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could

7. This tells me a ton about password crackers and how important it is to have a strong password. For the two easy passwords we experimented with, it was almost instant to crack these passwords, but for the very complex password I entered in, the password

cracker could not decipher the hash value that was associated with the complex password.