Fundamentals of Information Security: Cybersecurity (88252)
Ana M Herrera Flores
Crypto Attacks

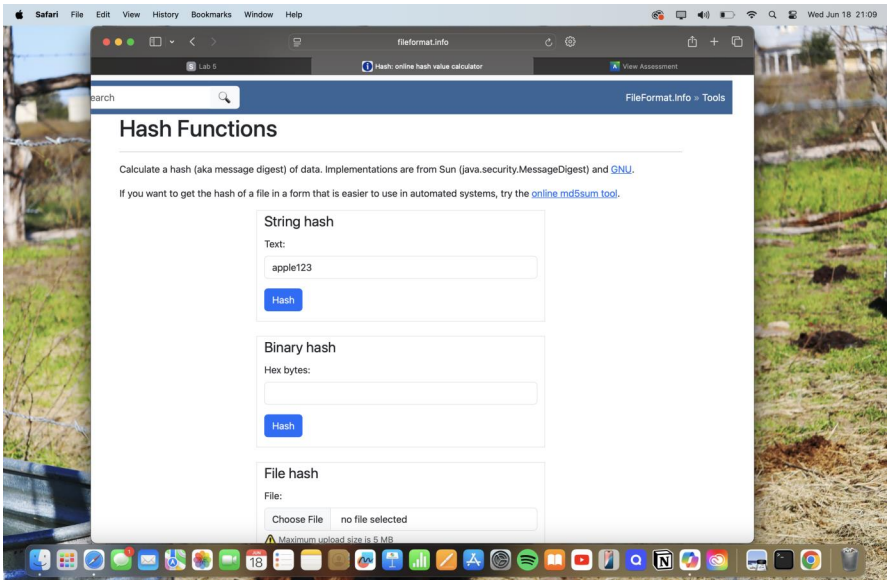
1. Create a password hash. Use a web browser to go to www.fileformat.info/tool/hash.htm
2. Under String Hash, enter the simple password apple123 in the Text: box.
3. Click Hash.
4. Scroll down the page and copy the MD4 hash of this password to your Clipboard by selecting the text, right-clicking and choosing Copy.
5. Open a new tab on your web browser. Go to https://crackstation.net/
6. Paste the MD4 hash of apple123 into the text box beneath Enter up to 10 non-salted hashes:
7. In the RECAPTCHA box, enter the current value being displayed in the box that says Type the text.

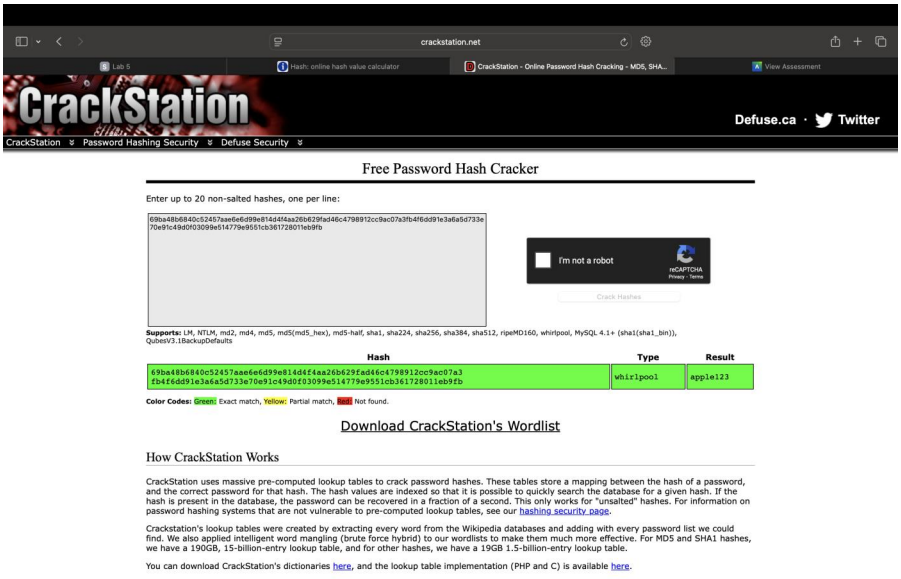
8. Click Crack Hashes.
• How long did it take the rainbow table to crack this hash?
1 second

10. Click the browser tab to return to FileFormat.Info.
11. Under String hash, enter the longer password 12applesauce in the Text: box.
12. Click Hash.
13. Scroll down the page and copy the MD4 hash of this password to your Clipboard.
14. Click browser tab to switch to the CrackStation site.
15. Paste the MD4 hash of 12applesauce into the text box beneath Enter up to 10 non-salted hashes:
16. In the RECAPTCHA box, enter the current value being displayed in the box that says Type the text.
17. Click Crack Hashes.
• How long did it take the rainbow table to crack this hash?
1 second

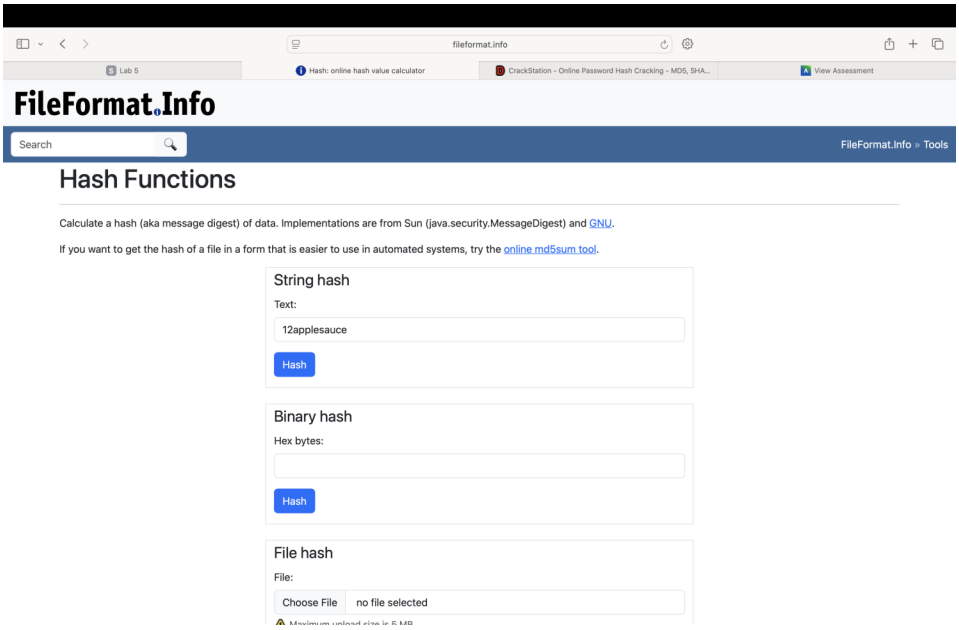
18. Try to do some other password cracks. Answer the question: What is more important the algorithm or the complexity of the password? Explain…
The complexity is more important; this means we should avoid common passwords patterns, making it harder for hackers to crack the password.
WHAT TO TURN-IN.
1) Show me screen shots that you have created hash values and cracked them.

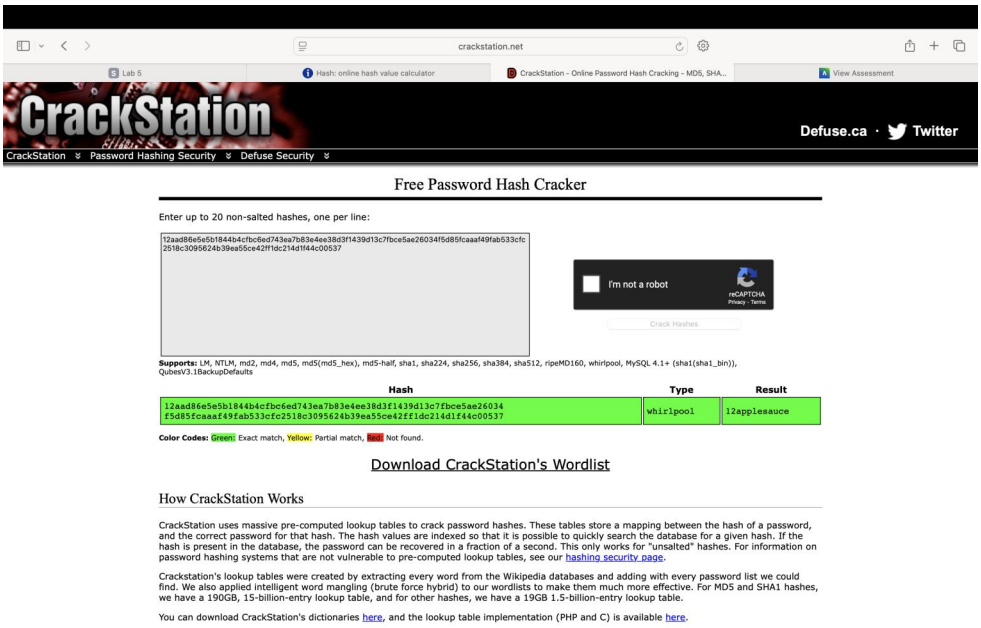
a. Explain the screen shots/snippets
2) Make sure you answer Question 18.



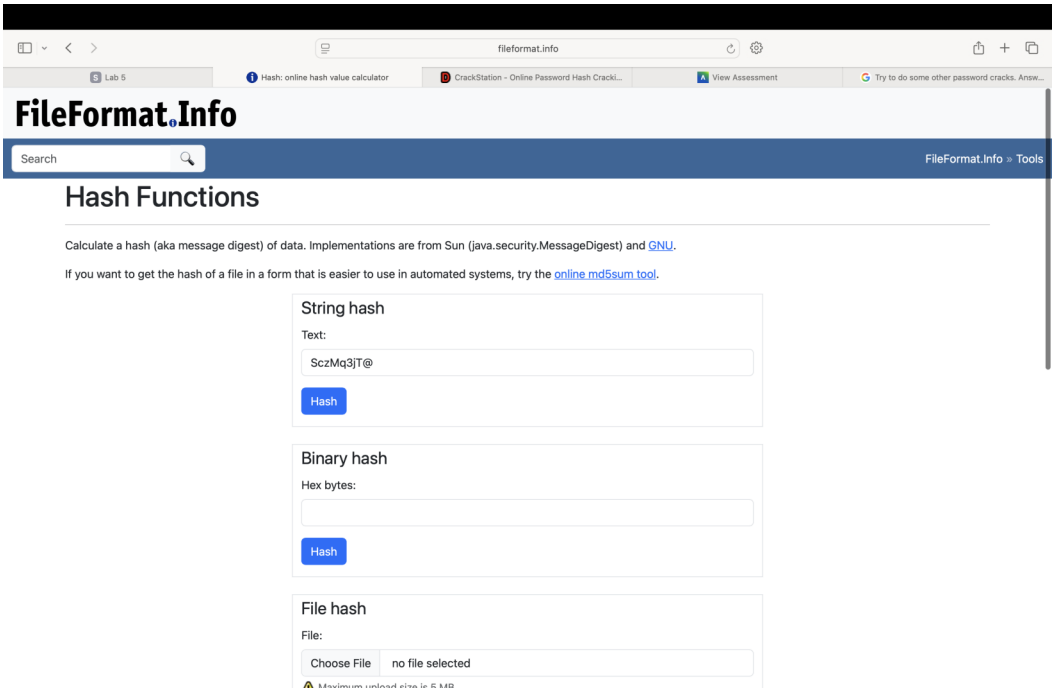


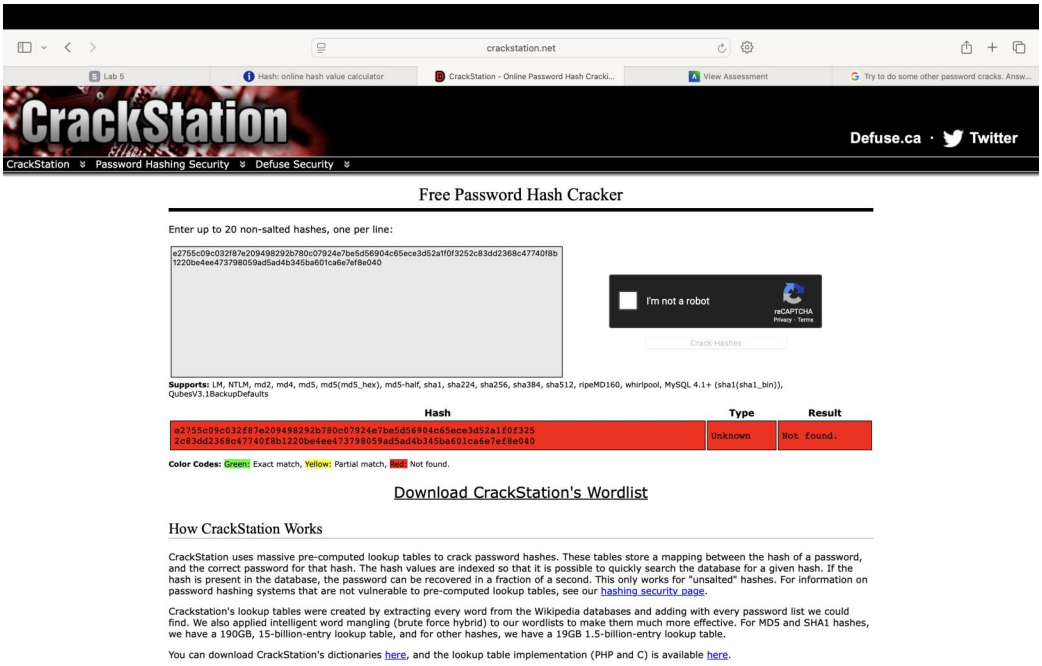
These 2 screenshots are for apple123 example, and we can see that we were able to obtain the password from the rainbow table.



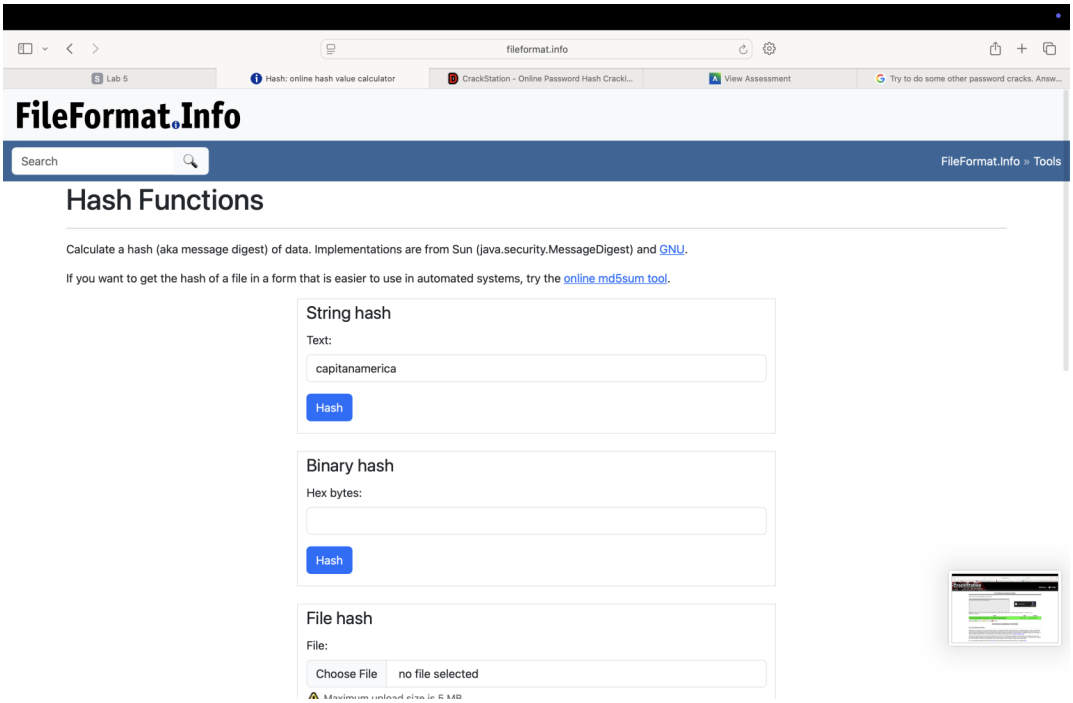


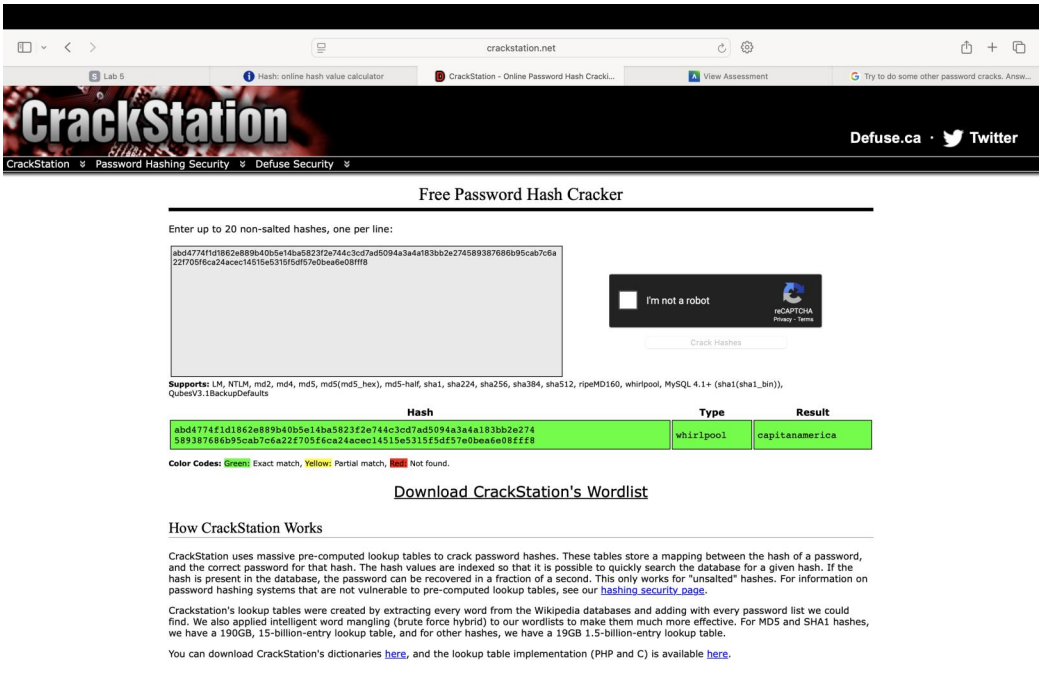
As in the previous example, these 2 pictures are also from the examples provided in class. This one is for 12applesauce. The rainbow table was also able to crack the password.





In these other 2 screenshots I introduced a password from an old wi-fi card that I used in Cuba. The password is not long, but it is a combination of upper and lower cases, numbers, and symbols. It doesn't mean anything, and the rainbow table was unable to crash into it.





This last example used the password capitanamerica. The rainbow table was able to crash the password in less than a second. The password is simple and refers to something that a lot of people know and use in their passwords.