Lab 3

COMP6035: Computer Security Principles



**Your Name**

Student #: R00201303

Date: 01.12.2021

Group: COMP1D-Y

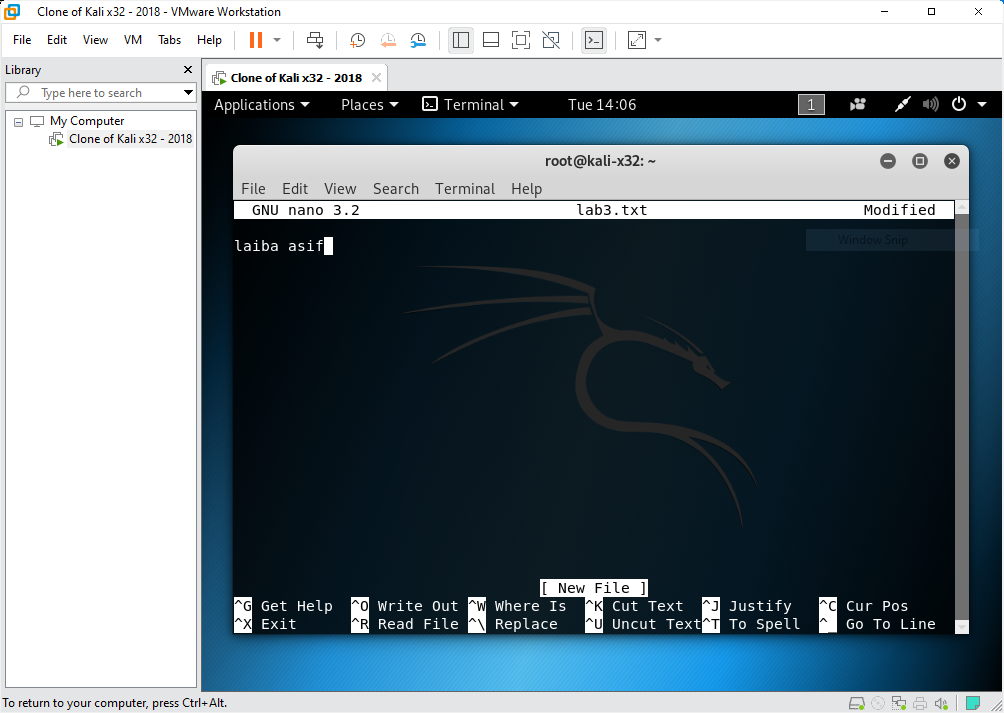
# 

# PART 1

# TASK 1:

Create new file screenshot(s) & observations:

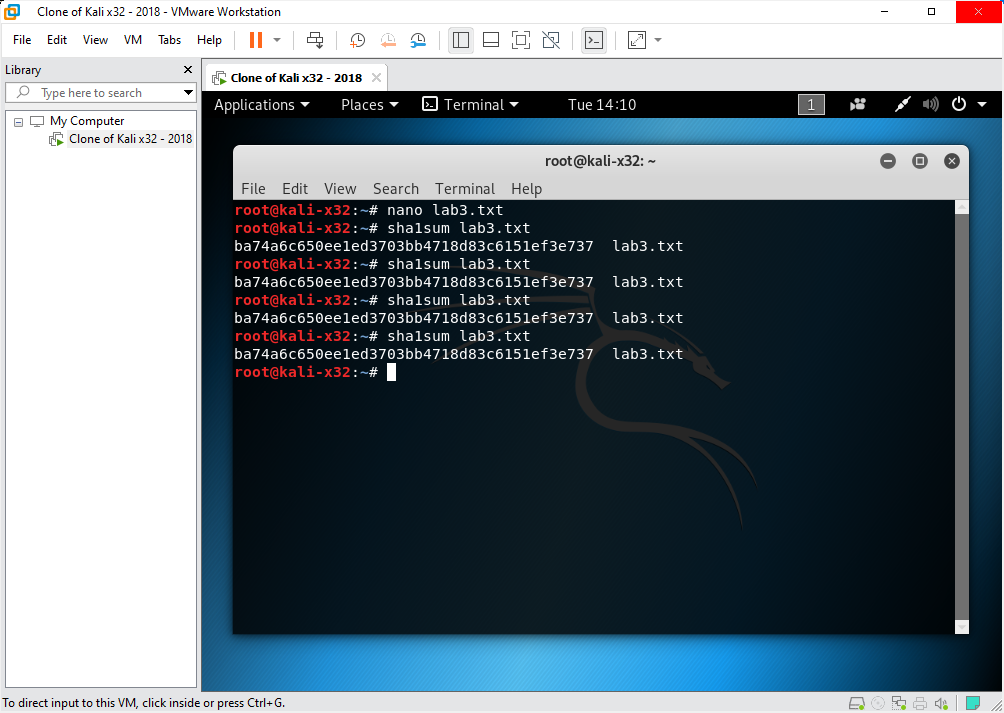
New file successfully created



# TASK 2:

Analyzing SHA1 hash of file screenshot(s) & observations:

The hash value is used to verify the integrity of a file. As a result, the whole reason for generating a hash value, namely to offer a unique measure for a file, has been called into question in the case of SHA1.

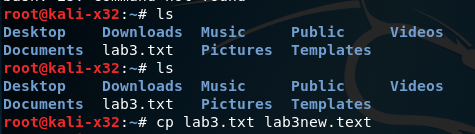


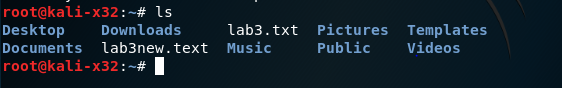
**QUESTION**: Is there a change in the hash value? What would happen if you repeated this step 10 times more? Explain your answer.

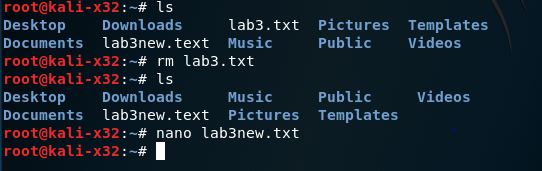
The hash value didn’t change so it doesn’t matter how many times you repeat this step even 10times.

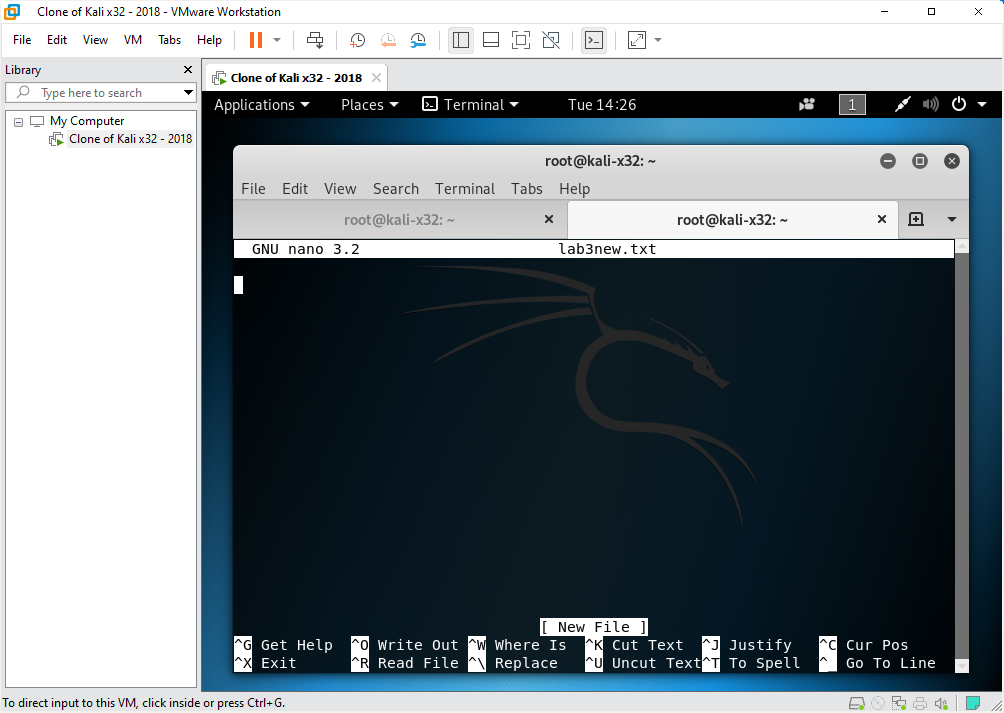
# TASK 3:

Analysing SHA1 hash when you change file title screenshot(s) & observations:











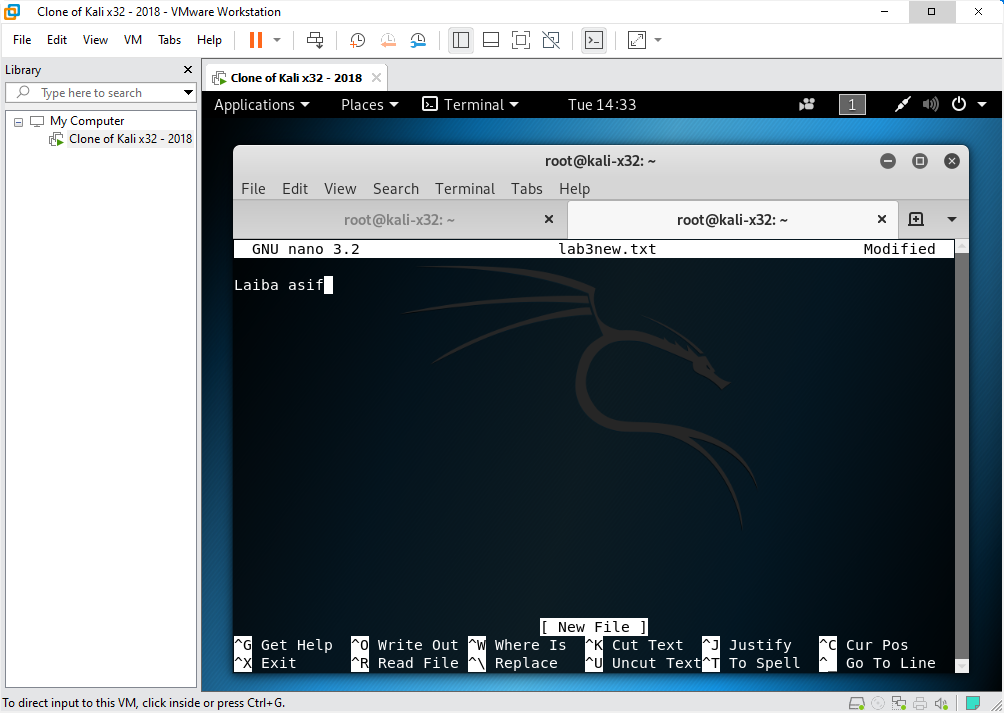
**QUESTION:** Has the hash changed? Explain your answer.

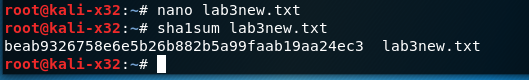
I don’t know but I didn’t got any hash value its says no such file but because a file's name is a system metadata value stored outside of the file in the master file table, changing the file's name or extension has no effect on the file's contents or hash value.

# TASK 4:

Analysing SHA1 hash when you change file contents screenshot(s) & observations:

Yes the hash value do change as the contents of a file are processed by a cryptographic algorithm, which generates a unique numerical value – the hash value – that uniquely identifies the file's contents. If the contents are changed in any way, the hash value will vary dramatically.





**QUESTION**: Has the hash changed? Explain your answer.

# 

# TASK 5:

Comparing SHA algorithms screenshot(s) & observations:

**QUESTIONS:**

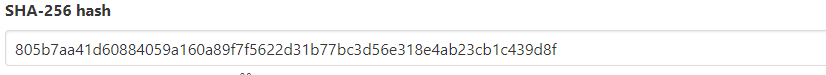
→ Research and explain the difference between SHA-1 and newer SHA algorithms (e.g. SHA-2, SHA-3).

SHA-1 is a 160-bit hash function that is like the MD5 technique. The National Security Agency (NSA) created this as part of the Digital Signature Algorithm. After SHA-1's cryptographic flaws were found, the standard was no longer authorized for most cryptographic applications after 2010.

SHA-2: A family of two comparable hash algorithms, SHA-256 and SHA-512, with varying block sizes. The word size of SHA-256 and SHA-512 is different; SHA-256 utilizes 32-bit bits and SHA-512 uses 64-bit words. Each standard also has shortened variants called SHA-224, SHA-384, SHA-512/224, and SHA-512/256. The National Security Agency (NSA) was also responsible for these.

SHA-3 is a hash function that was previously known as Keccak and was chosen in 2012 following a public competition among non-NSA inventors. It uses the same hash lengths as SHA-2 and has a different internal structure than the rest of the SHA family.

→ Calculate the SHA256 hash and record the hash value in your report.



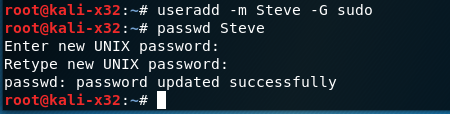
# 

# PART 2

# TASK 1:

Create user account for Steve screenshot(s) & observations:

The sudo (superuser do) group is added to the account using the -G switch.



# TASK 2:

Create your own user account screenshot(s) & observations:

User added successfully

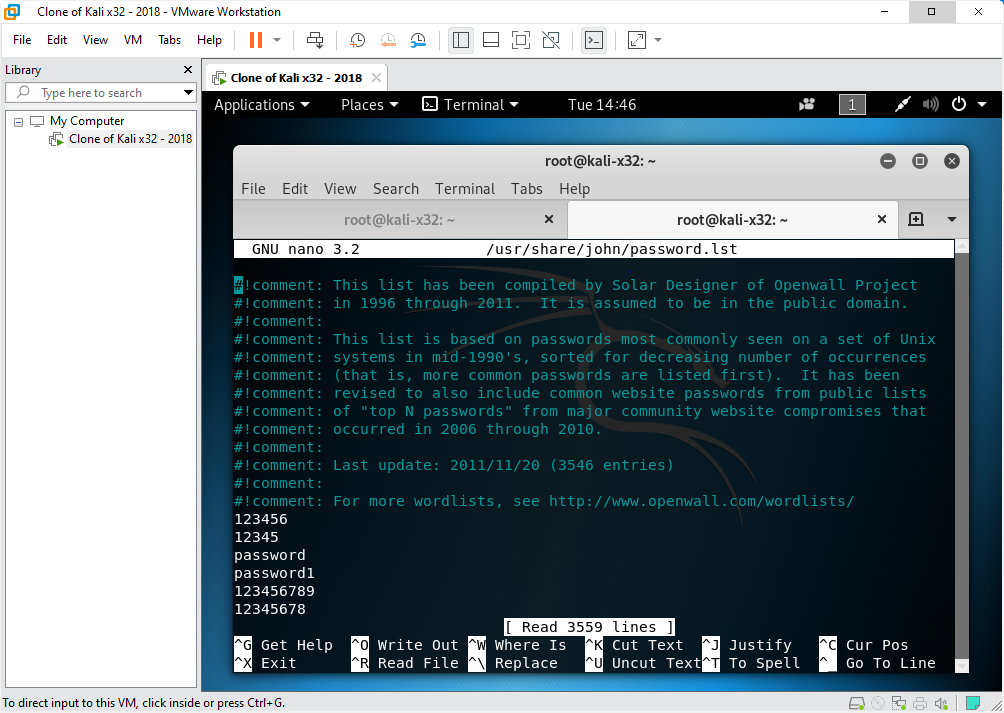
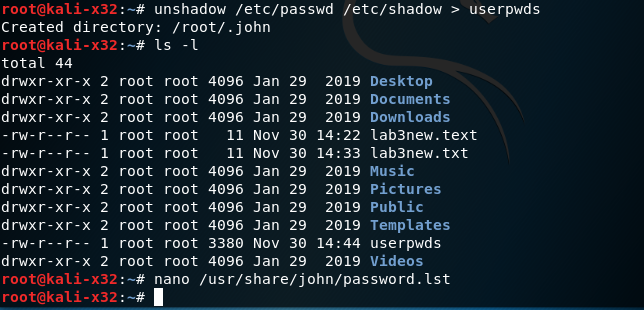


# 

# TASK 3:

Use unshadow to create a file with username and password details screenshot(s) & observations:

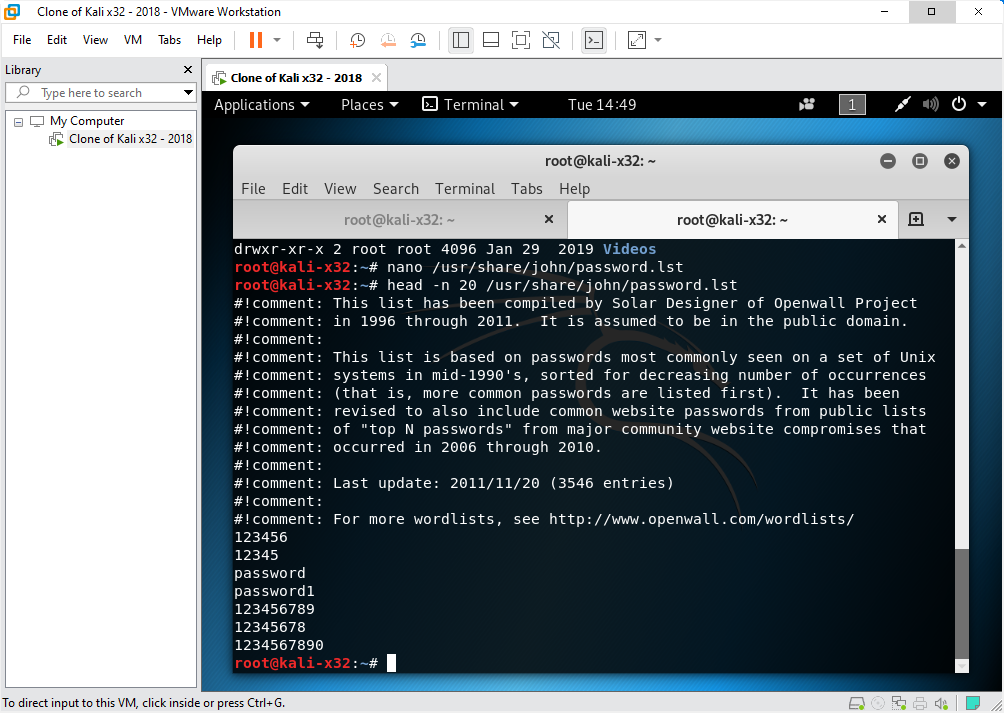
The /etc/shadow file contains the actual password for the user's account in encrypted format (more like a hash of the password) as well as extra attributes relevant to the user password.



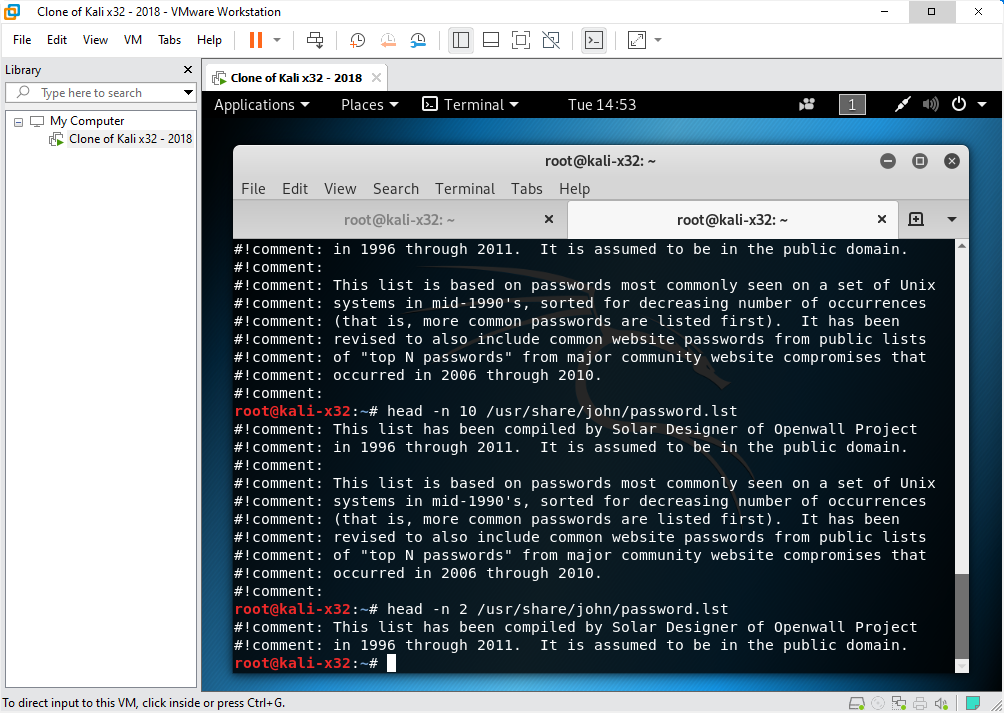
# TASK 4:

View only specific parts of file screenshot(s) & observations:

Only a portion of the file may be viewed.







**QUESTIONS:** Include your answers and a screenshot in your report for the following questions.

What happens if you remove -n 20 from the previous command and run it again?

Only comments can be viewed

Modify this command to view the last 10 lines of the password.lst file? (Hint: what is the opposite to head?)

Only 10 lines can be viewed

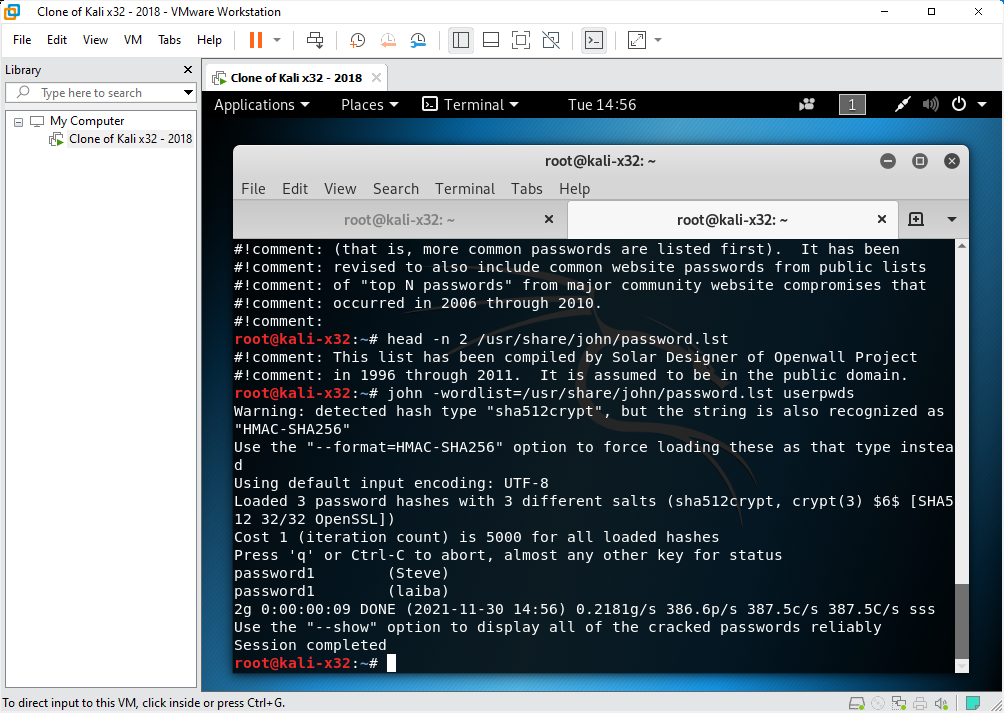
Modify this command to only view the last 2 lines of the password.lst file.

# 

# TASK 5:

Crack the password screenshot(s) & observations:

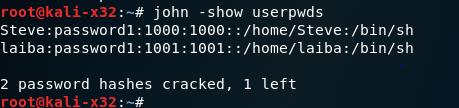
Warning to detect the type of hash

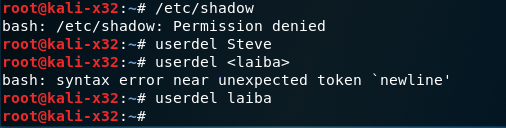


# TASK 6:

Show the details of the user accounts which includes the password screenshot(s) & observations:

2 hash passwords cracked and both Steve and laiba user deleted



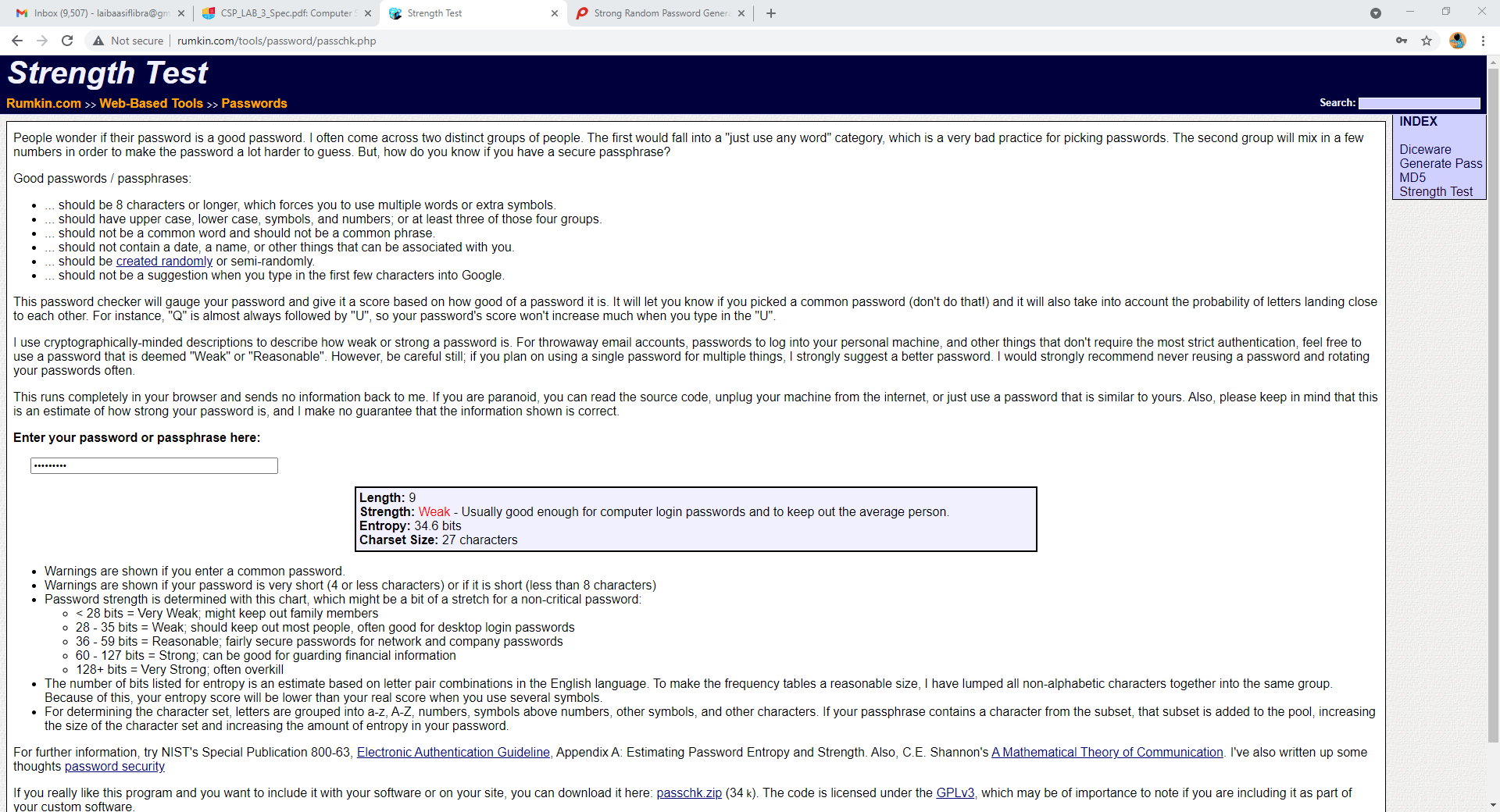


# PART 3

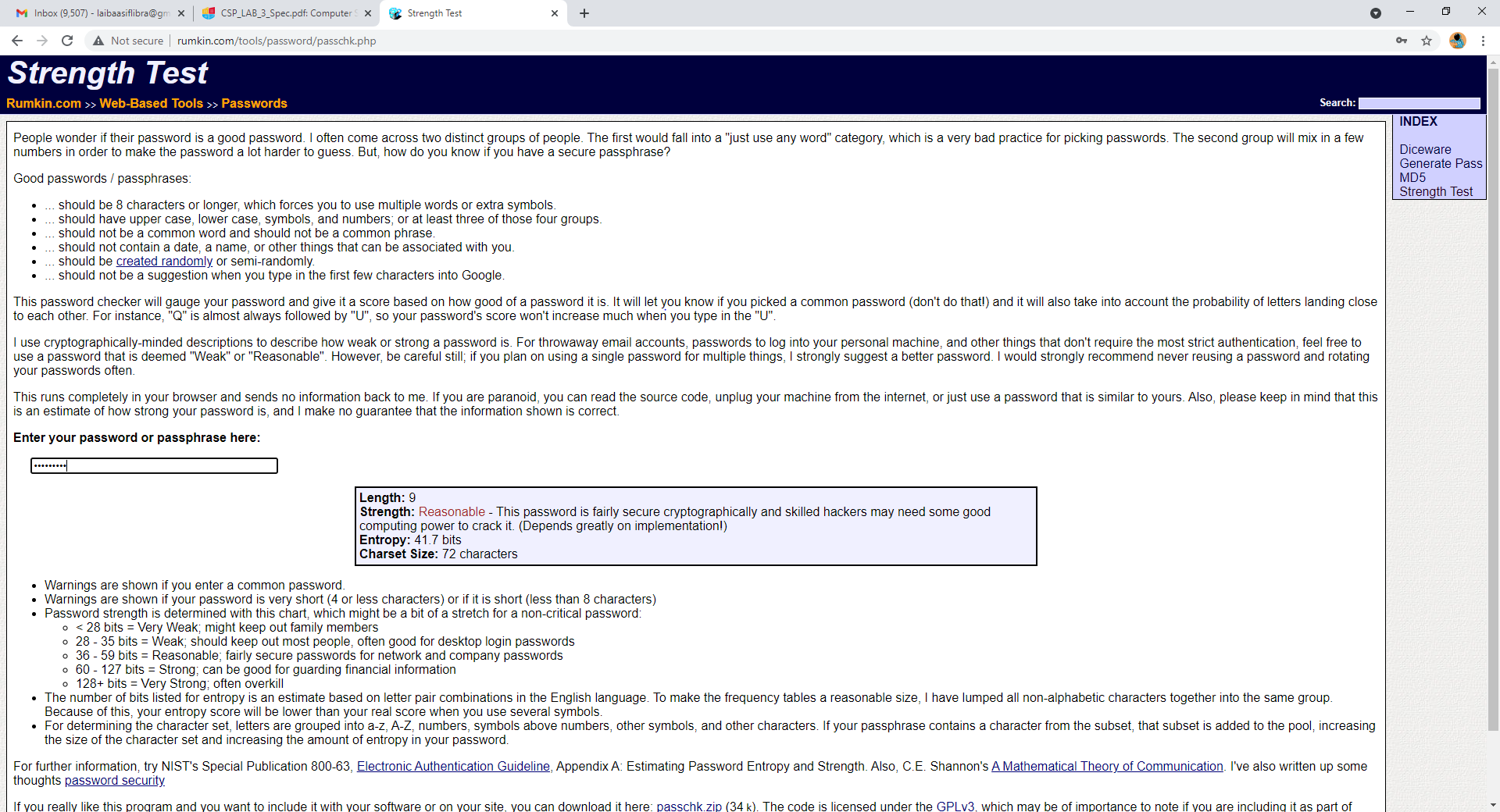
# TASK 1:

Create passwords and check password strength using online tool screenshot(s) & observations:

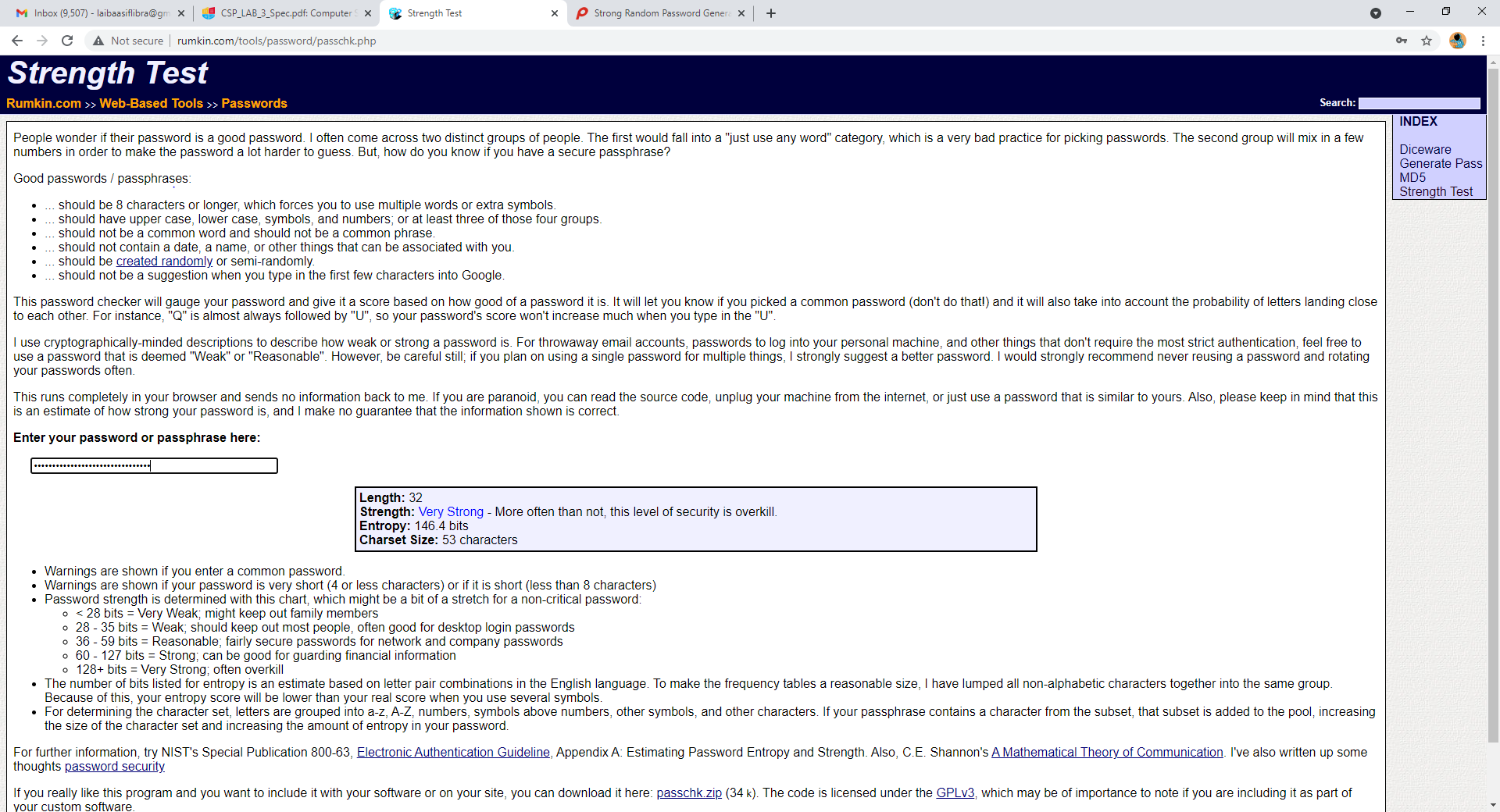
Password: abcdefgh (weak password)



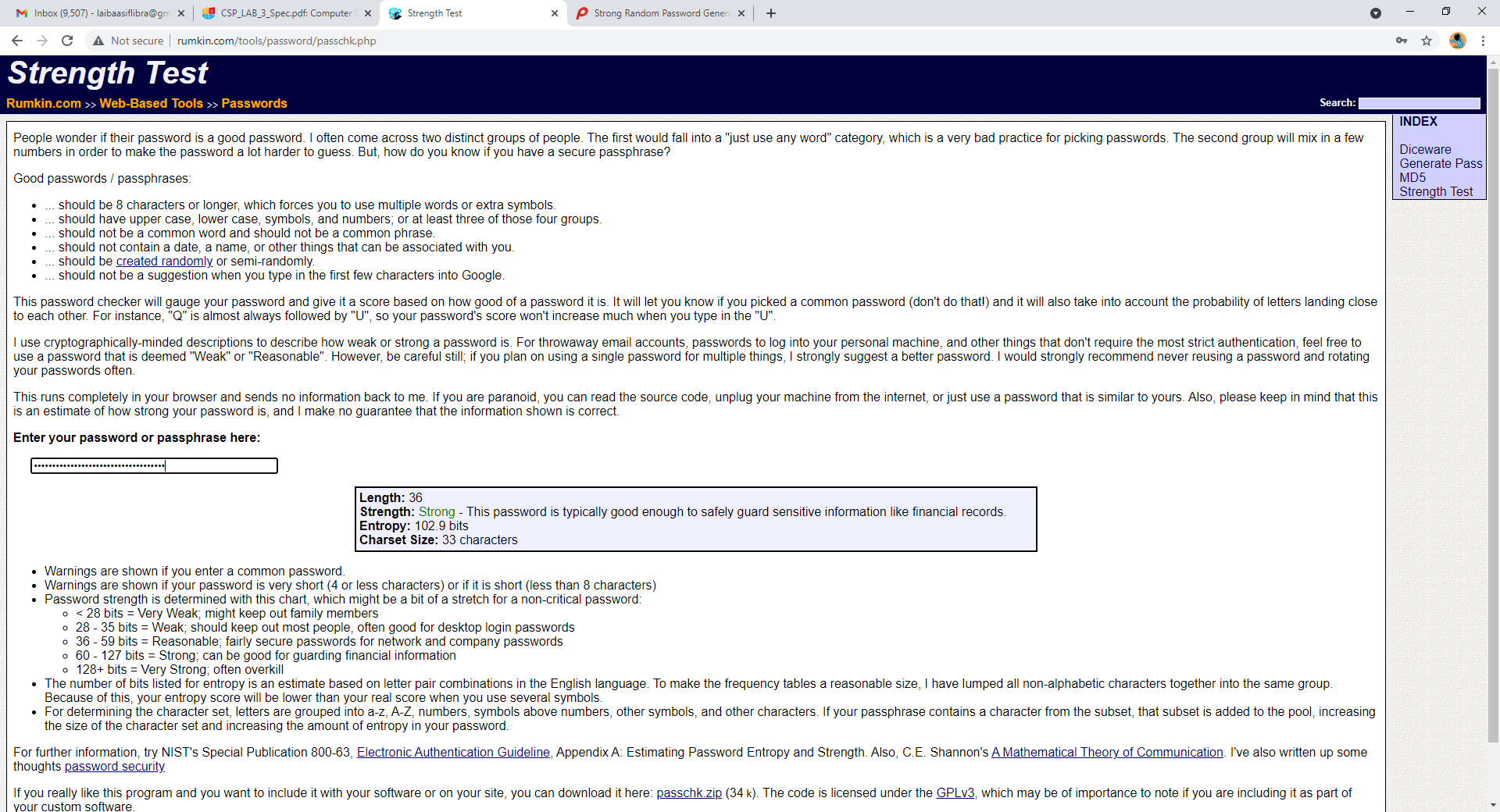
Password:  #Rajput12 (reasonable password)



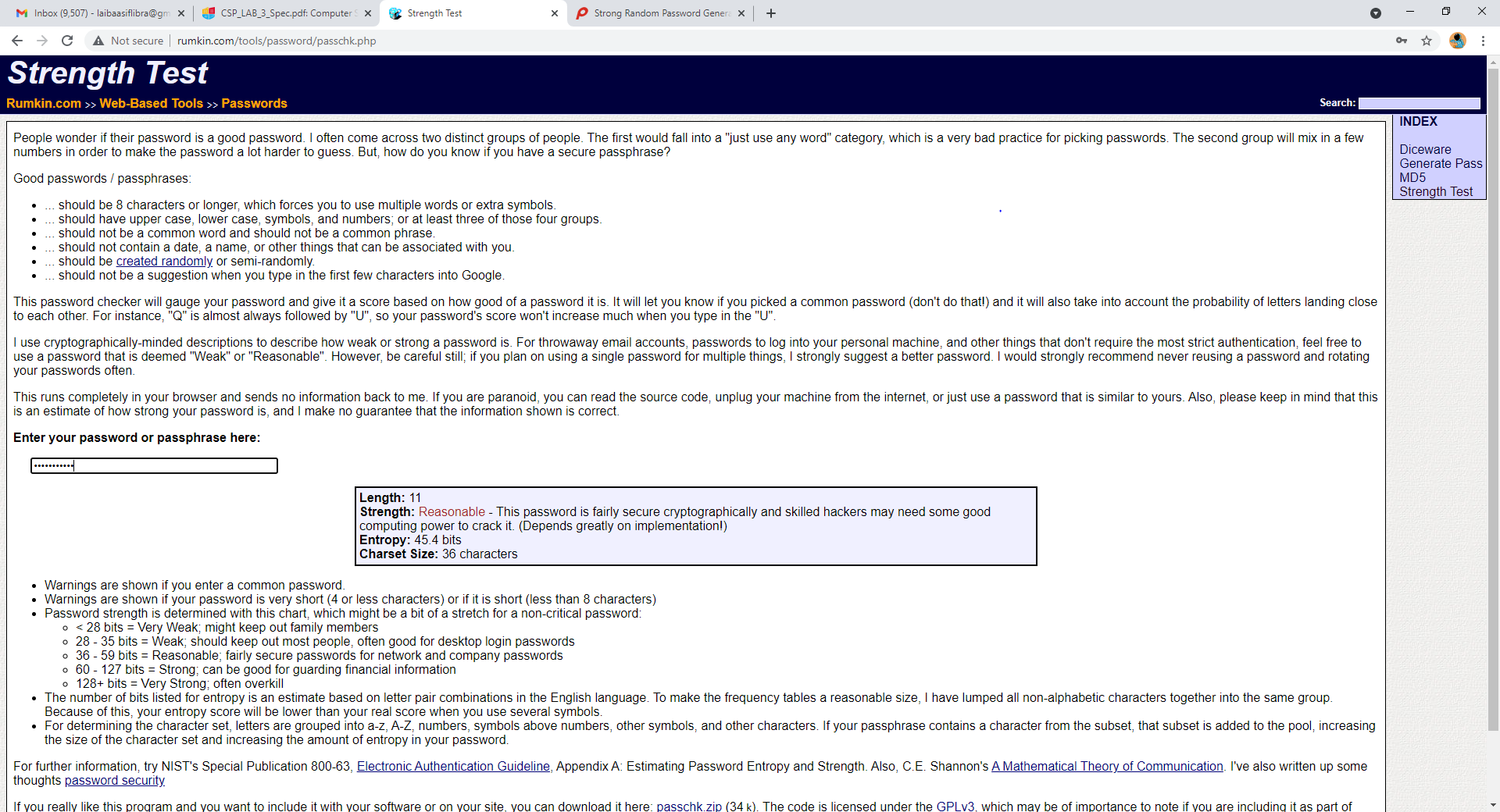
Password: do NOT send across the Internet (very strong password)



Password: { } [ ] ( ) / \ ' " ` ~ , ; : . < > (strong password)

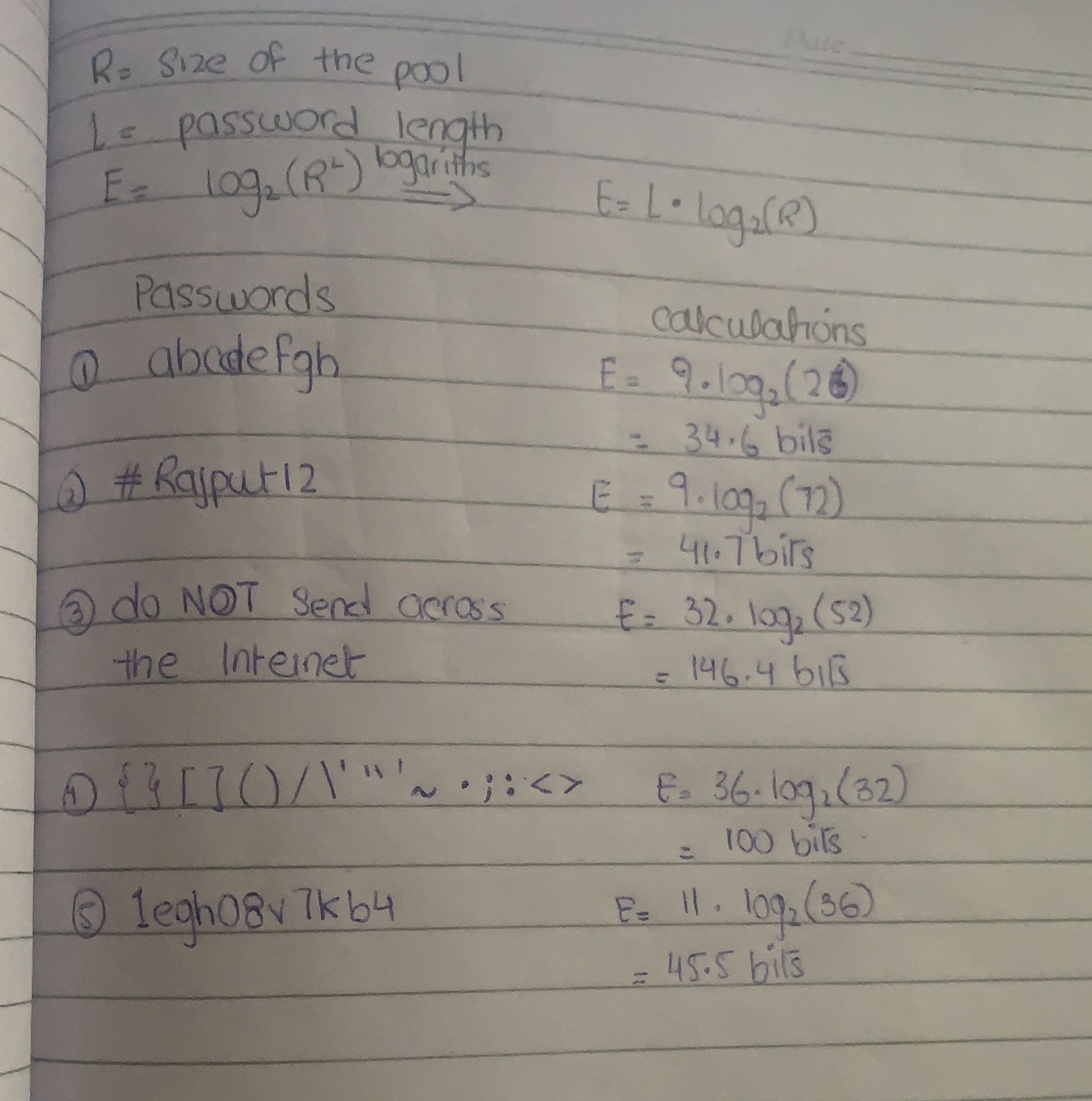


Password: 1e8h0g7vkb4 (reasonable password)



# TASK 2:

Password entropy calculation (show calculations):

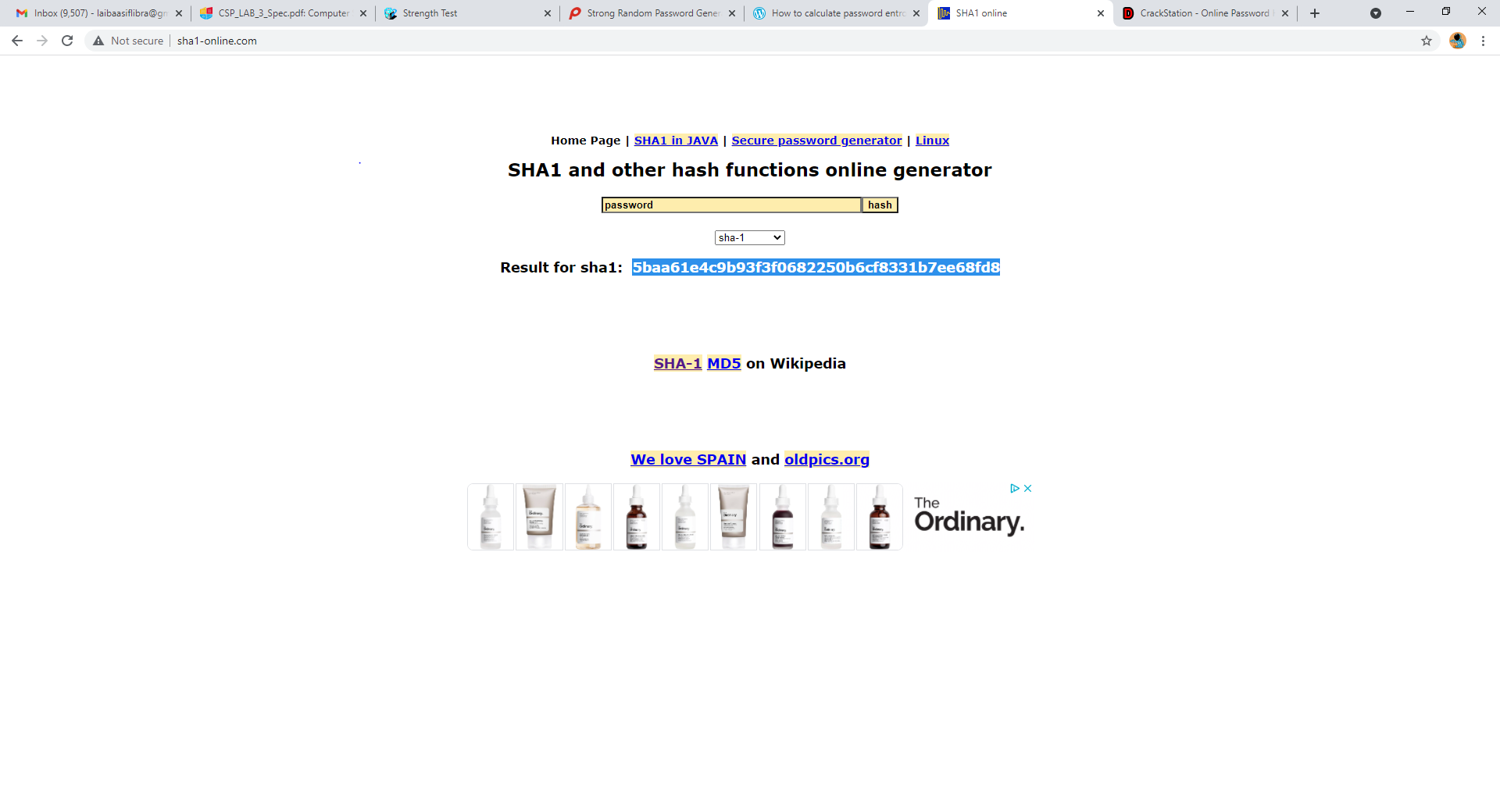


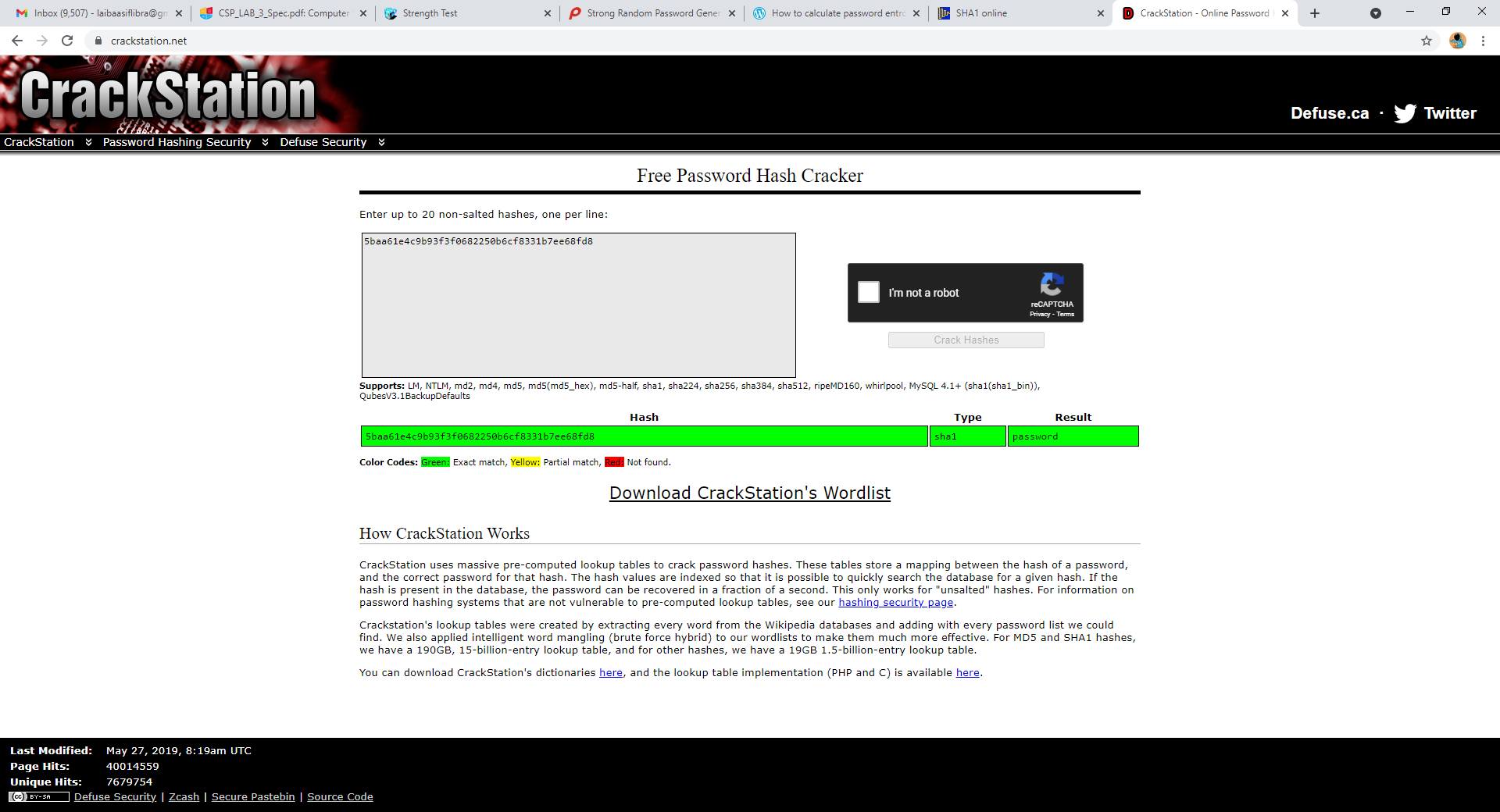
# PART 4

# TASK 1:

Crack hash of weak password screenshot(s) & observations:

Cracked type: SHA1 and result: password

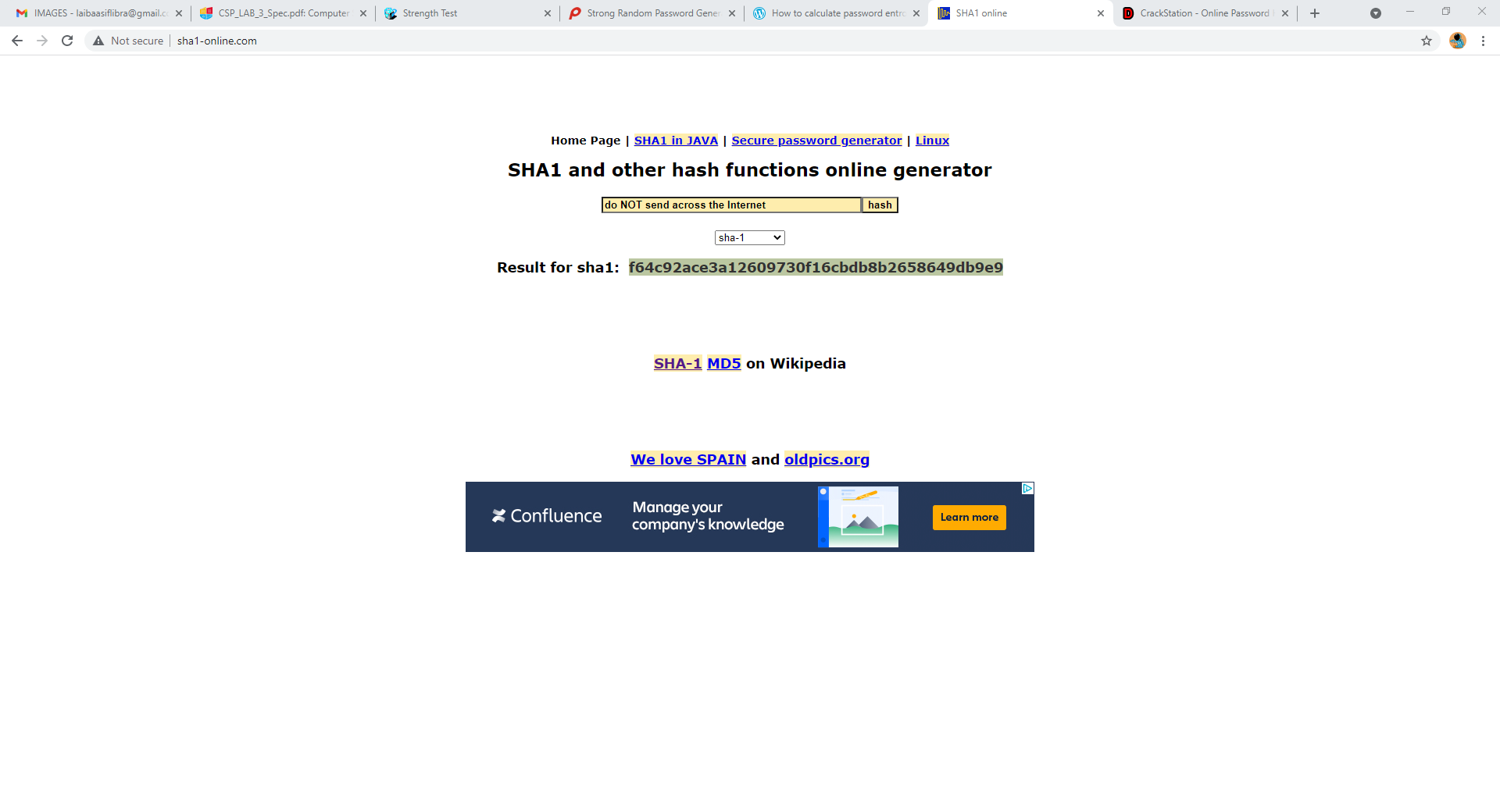




# TASK 2:

Try to crack hash of stronger password screenshot(s) & observations:

Not Cracked type: unknown and result: not found



# 

# Conclusion

Summarise what you have learned in the lab. This is an important and significant part of completing lab work.

A hash value is a numeric value with a specified length that uniquely identifies data. With digital signatures, hash values are used to represent large amounts of data as much smaller numeric values. A hash value can be signed more quickly than a larger value. Data received via unprotected networks can also be checked for integrity using hash values. It's a word you'll hear a lot while you're downloading software. Before downloading new software from a credible source, compute the hash of the downloaded file and compare it to the hash supplied on the trustworthy website. If the calculated hash matches the published hash, you may trust that the file's integrity has been preserved. Compare the hash value of received data to the hash value of data as it was provided to see if data has been modified.