Quantitative Usability Evaluations - Project 2

Victorious Purple Hackers

Esti Tweg - 101005024

Jordan Li - 100974153

Shaan Malik - 101036858

Jeremy DenHartogh - 100968279

COMP 3008 A

April 9, 2019

https://github.com/JeremyDenHartogh/Comp3008Project2

Part 1 - Descriptive Statistics

Advantages of Image Scheme

- Order doesn’t matter when entering password, easier to remember
    - More forgiving
- Password can be remembered as a series of coordinates
- Takes advantage of recognition, can recognize certain parts of image as parts of password
- Helpful for more “visual learners”

Disadvantages of Image Scheme

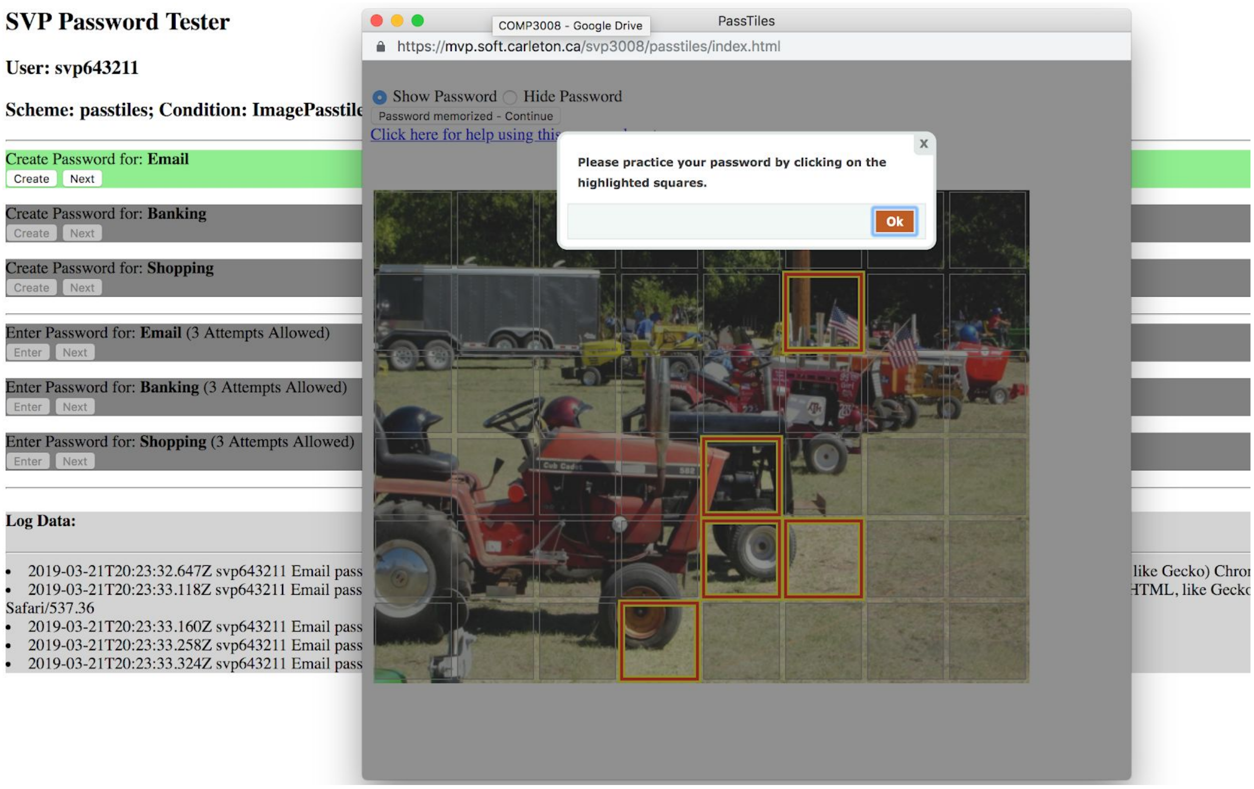
- Order doesn’t matter when entering password, therefore password space is smaller, making the password less safe
- Difficult to remember location
- Feels difficult to remember 5 different places to click
- Images and locations to click on images have no significance to user
    - Makes more difficult to remember
- Difficult to write down to remember and refer to later

Advantages of Text Scheme

- Only have to remember a short string of characters (5 characters)
- Larger password space, therefore passwords are safer
- Easy to write down to refer to later

Disadvantages of Text Scheme

- Assigned textual password is made up of seemingly random characters that are hard to remember
- If you use this method for multiple passwords, it will be tough to remember them. Even if you do remember the password, you may not remember what it’s used for.
- No significance or meaning of assigned password string
- Not easy to remember string using grouping technique due to characters being random



SVP Password Tester

User: svp643211

Scheme: passtiles; Condition: ImagePasstile

Create Password for: **Email**

Create Password for: **Banking**

Create Password for: **Shopping**

Enter Password for: **Email** (3 Attempts Allowed)

Enter Password for: **Banking** (3 Attempts Allowed)

Enter Password for: **Shopping** (3 Attempts Allowed)

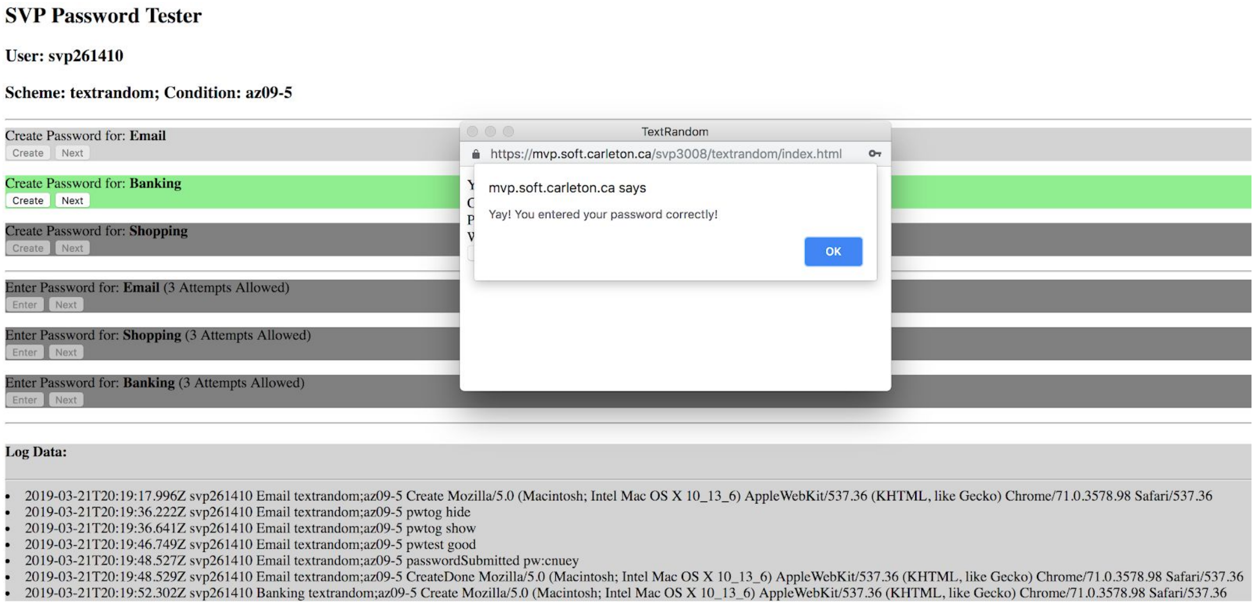
Log Data:

```
• 2019-03-21T20:23:32.647Z svp643211 Email pass                              like Gecko) Chro
• 2019-03-21T20:23:33.118Z svp643211 Email pass                              HTML, like Gecko
Safari/537.36
• 2019-03-21T20:23:33.160Z svp643211 Email pass
• 2019-03-21T20:23:33.258Z svp643211 Email pass
• 2019-03-21T20:23:33.324Z svp643211 Email pass
```

Please practice your password by clicking on the highlighted squares.

COMP3008 - Google Drive
PassTiles
https://mvp.soft.carleton.ca/svp3008/passtiles/index.html
● Show Password ○ Hide Password
Password memorized - Continue
Click here for help using this
x
Ok
Create
Next
Enter

Figure 1: Learning the assigned image password



SVP Password Tester

User: svp261410

Scheme: textrandom; Condition: az09-5

Create Password for: **Email**

Create Password for: **Banking**

Create Password for: **Shopping**

Enter Password for: **Email** (3 Attempts Allowed)

Enter Password for: **Shopping** (3 Attempts Allowed)

Enter Password for: **Banking** (3 Attempts Allowed)

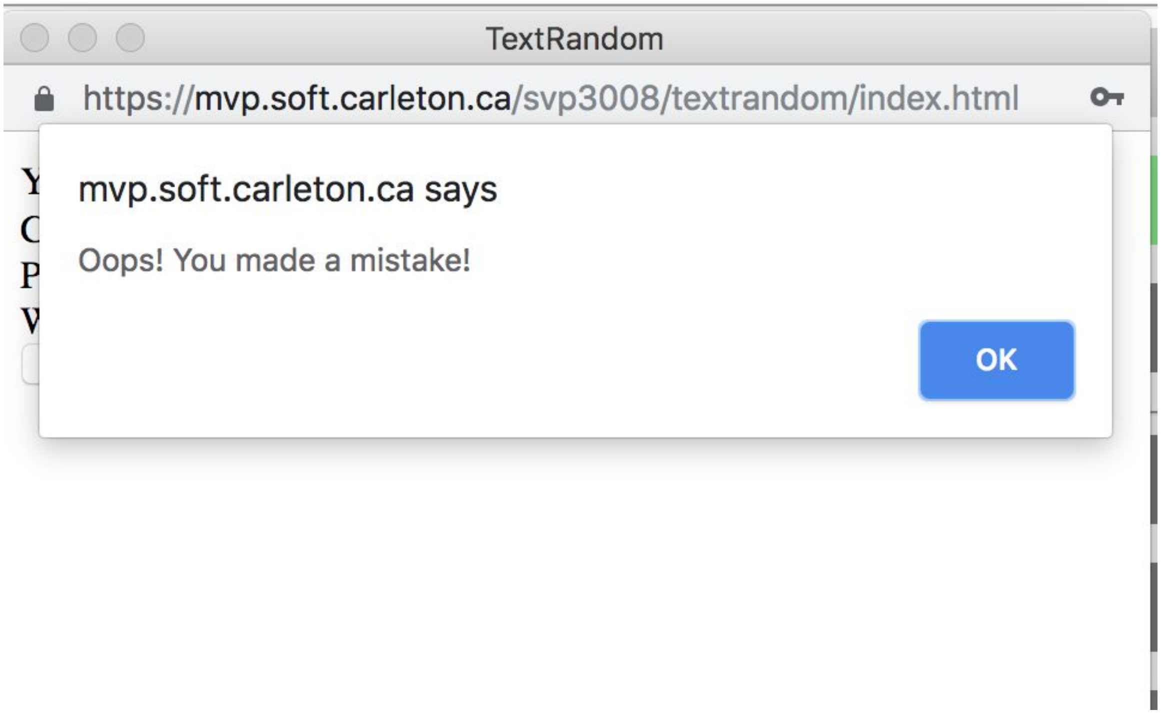
mvp.soft.carleton.ca says

Yay! You entered your password correctly!

Log Data:

```
• 2019-03-21T20:19:17.996Z svp261410 Email textrandom;az09-5 Create Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
• 2019-03-21T20:19:36.222Z svp261410 Email textrandom;az09-5 pwtog hide
• 2019-03-21T20:19:36.641Z svp261410 Email textrandom;az09-5 pwtog show
• 2019-03-21T20:19:46.749Z svp261410 Email textrandom;az09-5 pwtest good
• 2019-03-21T20:19:48.527Z svp261410 Email textrandom;az09-5 passwordSubmitted pw:cnuey
• 2019-03-21T20:19:48.529Z svp261410 Email textrandom;az09-5 CreateDone Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
• 2019-03-21T20:19:52.302Z svp261410 Banking textrandom;az09-5 Create Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
```

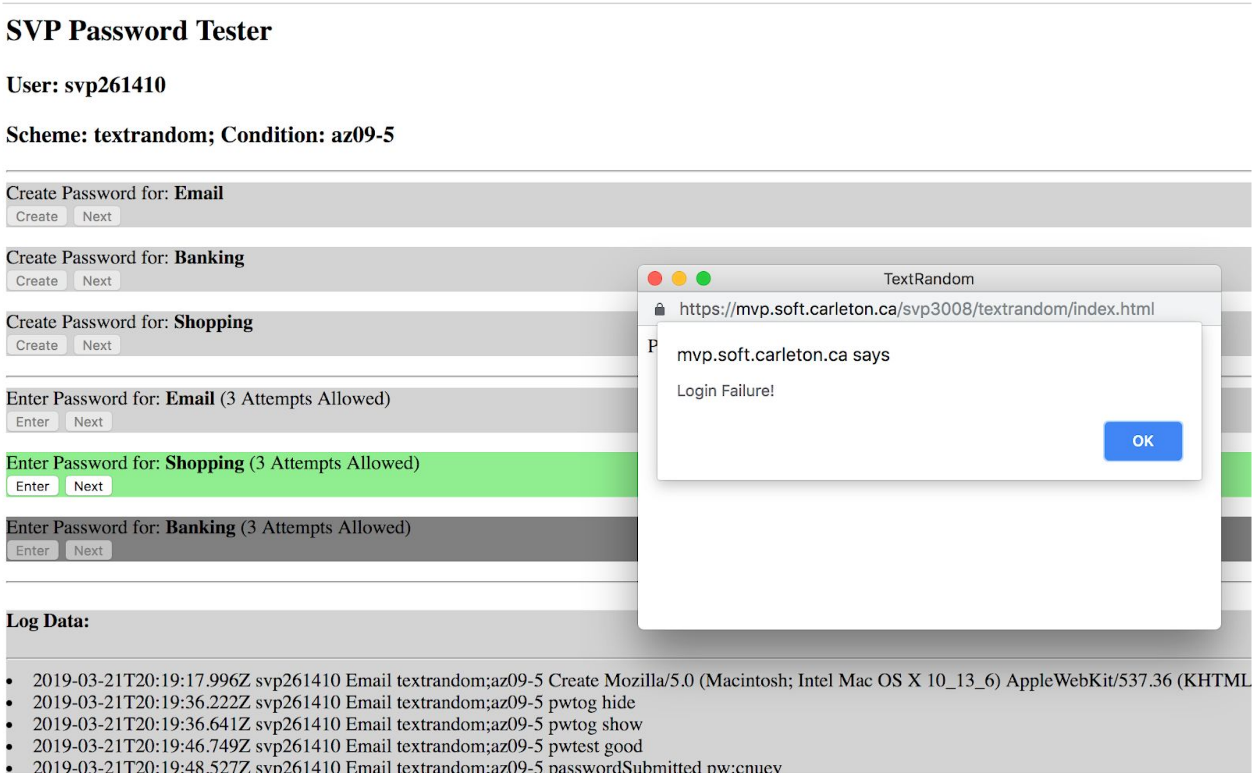
Figure 2: Correctly entered the assigned textual password



mvp.soft.carleton.ca says

Oops! You made a mistake!

Figure 3: Incorrectly entered the assigned text password



SVP Password Tester

User: svp261410

Scheme: textrandom; Condition: az09-5

Create Password for: **Email**

Create Password for: **Banking**

Create Password for: **Shopping**

Enter Password for: **Email** (3 Attempts Allowed)

Enter Password for: **Shopping** (3 Attempts Allowed)

Enter Password for: **Banking** (3 Attempts Allowed)

mvp.soft.carleton.ca says

Login Failure!

Log Data:

```
• 2019-03-21T20:19:17.996Z svp261410 Email textrandom;az09-5 Create Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML
• 2019-03-21T20:19:36.222Z svp261410 Email textrandom;az09-5 pwtog hide
• 2019-03-21T20:19:36.641Z svp261410 Email textrandom;az09-5 pwtog show
• 2019-03-21T20:19:46.749Z svp261410 Email textrandom;az09-5 pwtest good
• 2019-03-21T20:19:48.527Z svp261410 Email textrandom;az09-5 passwordSubmitted pw:cnuev
```

Figure 4: Unable to login due to incorrect password

Pseudocode

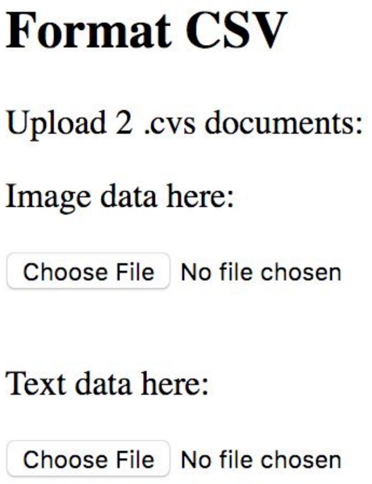
```
imageDataString = Import imageCSV from file reader
textDataString = Import textCSV from file reader

data = []//scheme (id, scheme,  numlogins, numSuccess, numFailed, successfulTime, failedTime

//format data
imageData = imageDataString split by "\n" and ","
imageUsers = []//User scheme: (id, scheme,  successfulLogins[], failedLogins[]

//store image data as users
for i 0->imageData.length
   if imageData[i][1] not in users
      User u = new User(imageData[i][1], "Image21", [], [])
      imageUsers.add(u)

   if imageData[i][6] == "badLogin"
      elapsedTime = subtractTime(imageData[i-1][0], imageData[i-2][0])
      imageUsers.get(imageData[i][1]).failedLogins.append(elapsedTime)

   else if imageData[i][6] == "goodLogin"
      elapsedTime = subtractTime(imageData[i-1][0], imageData[i-2][0])
      imageUsers.get(imageData[i][1]).successfulLogins.append(elapsedTime)

//repete for text data
//change strings for bad and good login and scheme to "Text21"


//combine data
for u in imageUsers
   line = []
   add u id, and scheme to line
   add total login attempts to line
   add number of successful logins attempts to line
   add number of failed logins attempts to line
```

Source Code

https://github.com/JeremyDenHartogh/Comp3008Project2/blob/master/Part1/formatData.js

Explanation of Data Cleaning Process

To clean the data, we decided to create a simple html interface where the image csv data and text csv data are uploaded. Once each csv file is uploaded, each unique user id is made into a user and stored. The user object has an id, scheme identifier, array of times for each successful login attempt and an array of times for each failed login attempt. Each of these values are derived from the uploaded csv file. Login times are retrieved by calculating the difference between timestamps for keywords representing the login attempts (“goodLogin” and “badLogin” for the image scheme, and “success” and “failure” for the text scheme). New users are created by the code reading a different username from the uploaded data. Next, we create a data array by iterating through each user and inserting a line object that contains the user id, scheme identifier, total number of login attempts, number of successful login attempts, number of failed login attempts, average time taken for each successful login attempt, and the average time taken for each failed login attempt. The data array is then converted into csv format. A link on the html page is displayed to download the newly generated csv file.



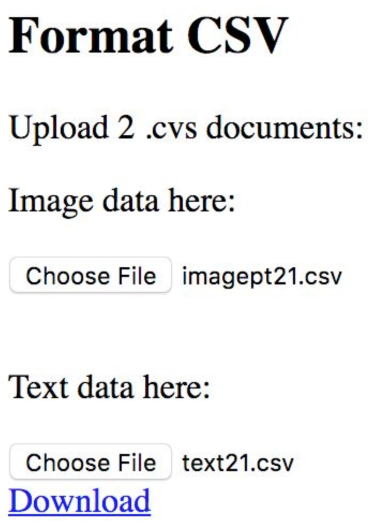
Format CSV

Upload 2 .cvs documents:

Image data here:

Text data here:

Figure 5: Html page before uploading csv documents



Format CSV

Upload 2 .cvs documents:

Image data here:

Choose File imagept21.csv

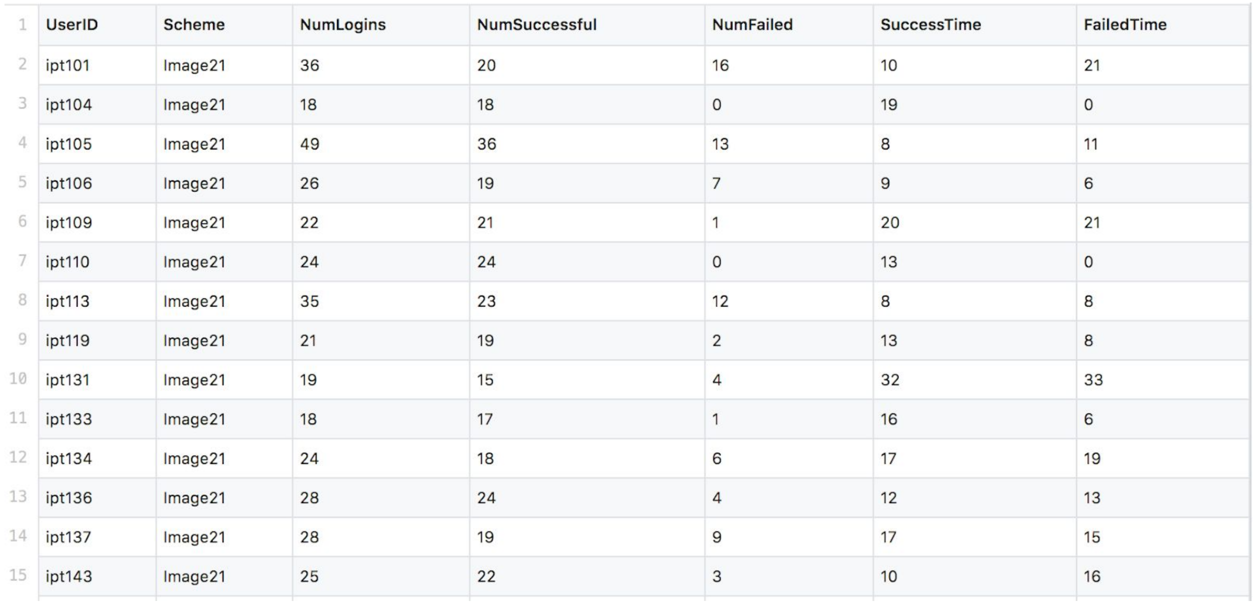
Text data here:

Choose File text21.csv

Download

Figure 6: Html page after uploading csv documents. Contains download link.

Resulting Data



UserID	Scheme	NumLogins	NumSuccessful	NumFailed	SuccessTime	FailedTime
ipt101	Image21	36	20	16	10	21
ipt104	Image21	18	18	0	19	0
ipt105	Image21	49	36	13	8	11
ipt106	Image21	26	19	7	9	6
ipt109	Image21	22	21	1	20	21
ipt110	Image21	24	24	0	13	0
ipt113	Image21	35	23	12	8	8
ipt119	Image21	21	19	2	13	8
ipt131	Image21	19	15	4	32	33
ipt133	Image21	18	17	1	16	6
ipt134	Image21	24	18	6	17	19
ipt136	Image21	28	24	4	12	13
ipt137	Image21	28	19	9	17	15
ipt143	Image21	25	22	3	10	16

Figure 7: Snapshot of resulting cleaned and formatted CSV file

Full CSV here:

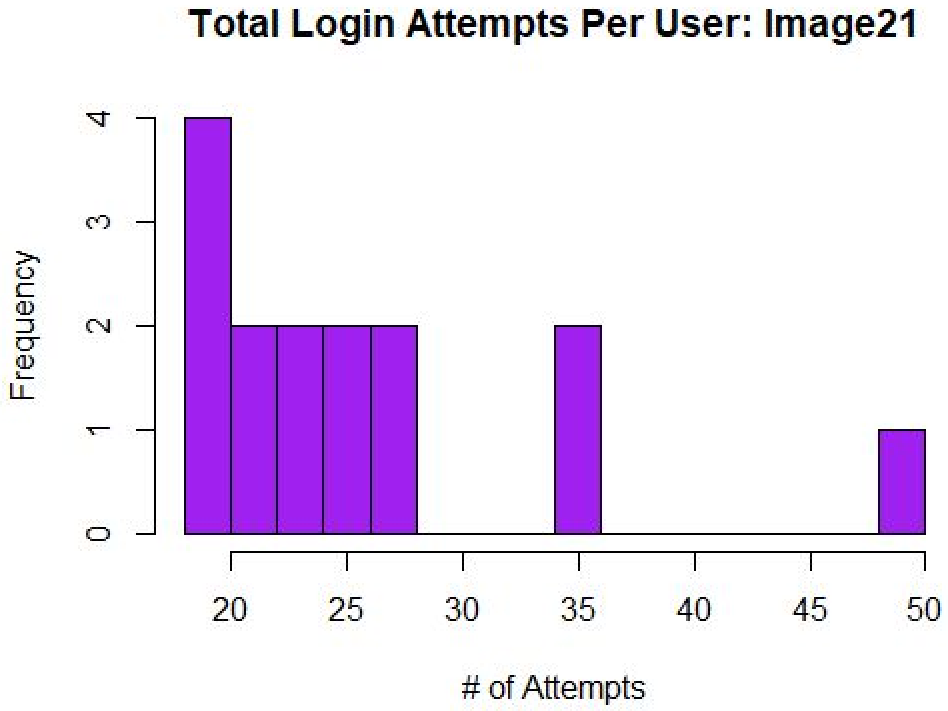
https://github.com/JeremyDenHartogh/Comp3008Project2/blob/master/Part1/data.csv

Descriptive Statistics of Data

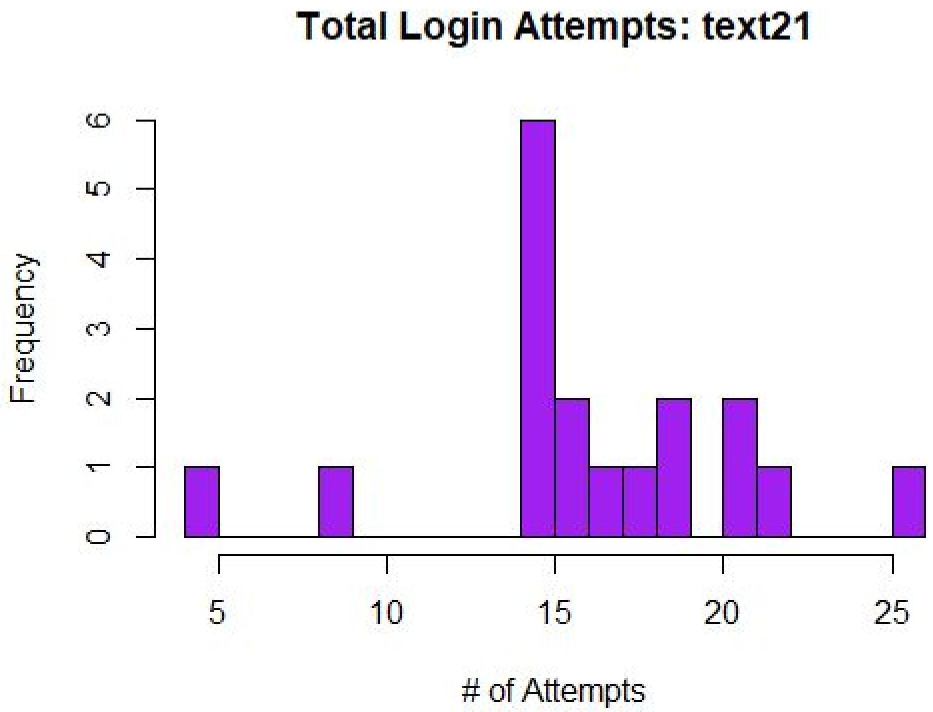
	Image Scheme	**Text Scheme**
Number of Total Login Attempts Mean	26.13	16.56
Number of Total Login Attempts Median	24	16
Number of Total Login Attempts Standard Deviation	8.43	4.87
Number of Successful Login Attempts Mean	20.87 (79.87%)	14 (84.54%)
Number of Successful Login Attempts Median	19	15
Number of Successful Login Attempts Standard Deviation	4.93	3.48
Number of Unsuccessful Login Attempts Mean	5.27 (20.17%)	2.56 (15.46%)
Number of Unsuccessful Login Attempts Median	4	1
Number of Unsuccessful Login Attempts Standard Deviation	5.12	3.33

Successful Login Time Mean	15.07	8.61
Successful Login Time Median	13	7.5
Successful Login Standard Deviation	6.49	3.20
Unsuccessful Login Time Mean	12.73	5.83
Unsuccessful Login Time Median	13	5
Unsuccessful Login Standard Deviation	8.73	6.73

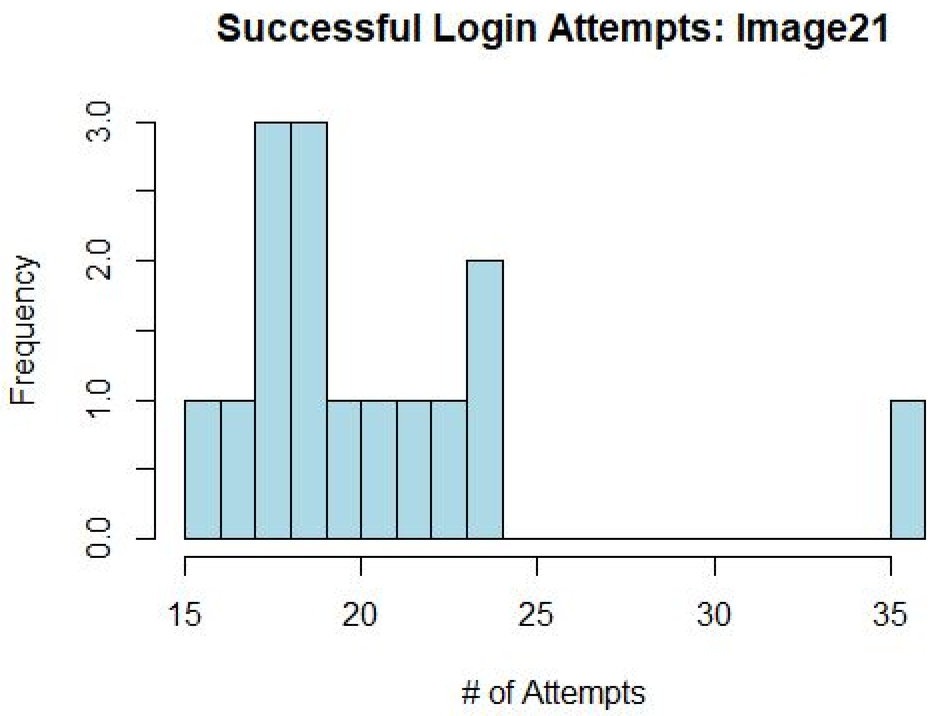
Mean, Median and Standard Deviations for number of login attempts (calculated in excel)



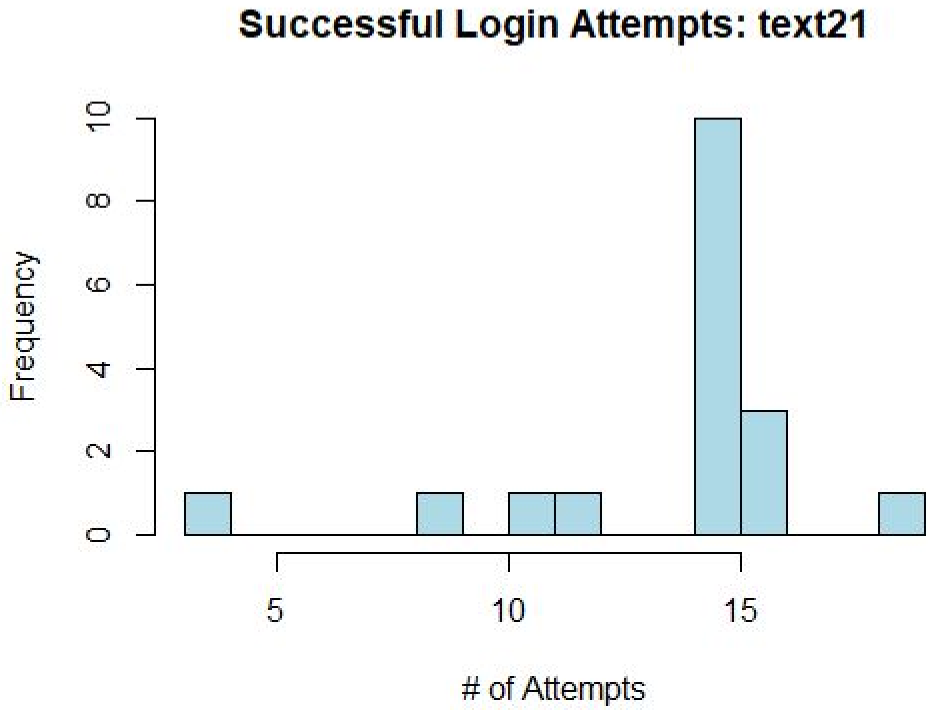
Number of Logins Histogram Image Password Scheme



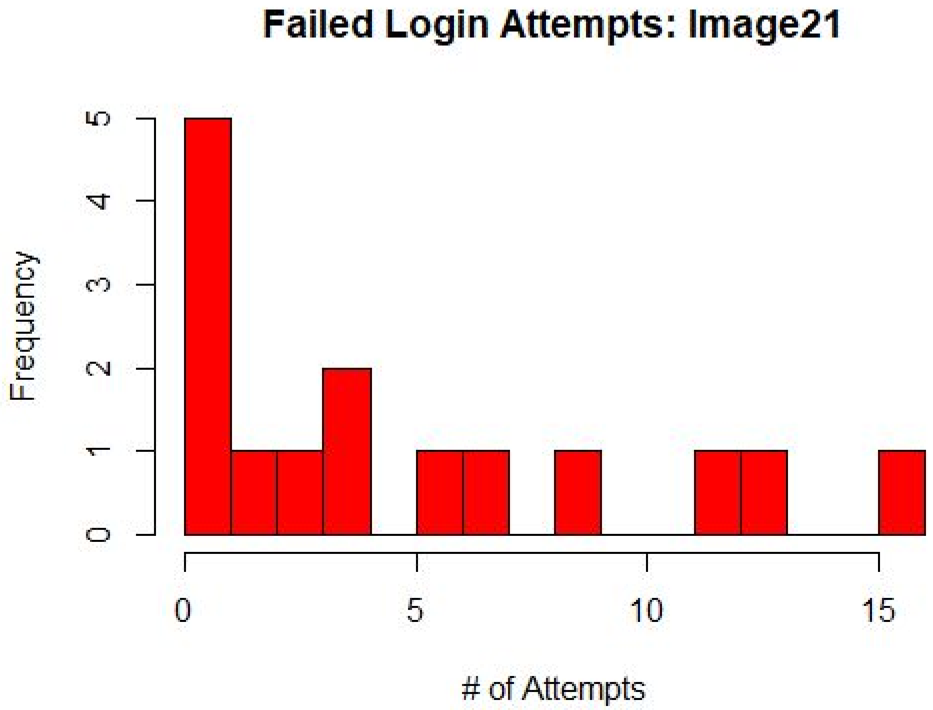
Number of Logins Histogram Text Password Scheme



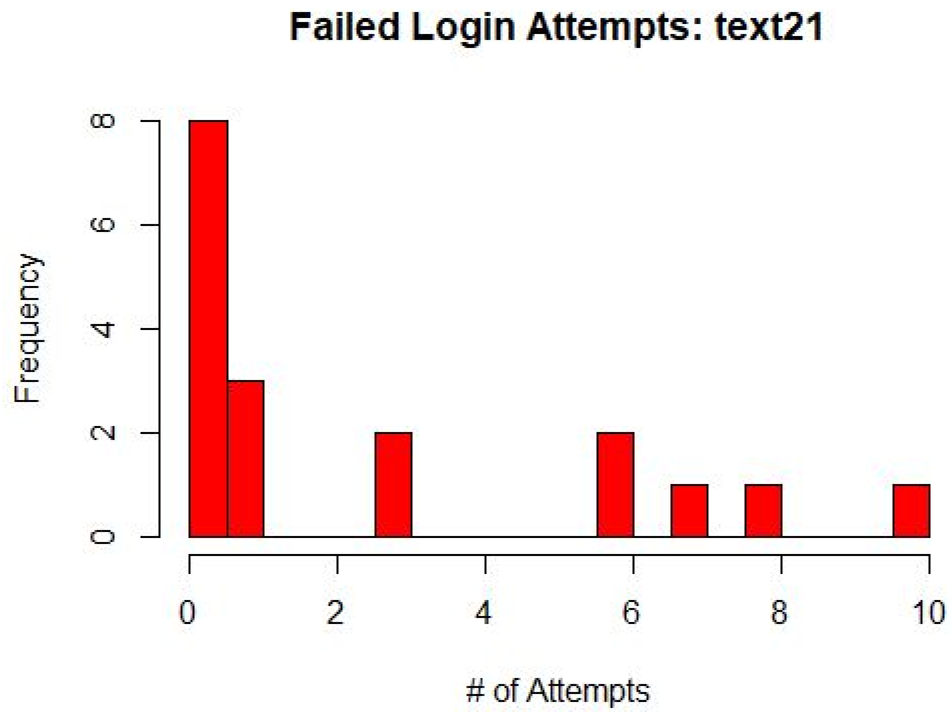
Number of Successful Logins Histogram Image Password Scheme



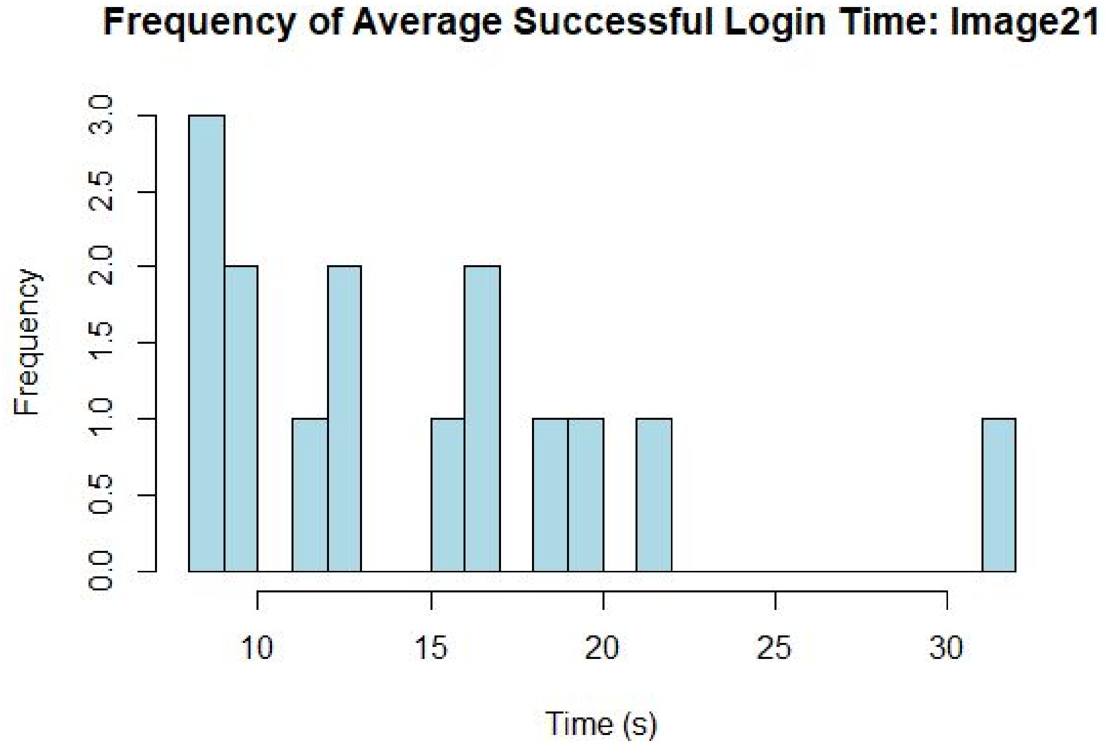
Number of Successful Logins Histogram Text Password Scheme



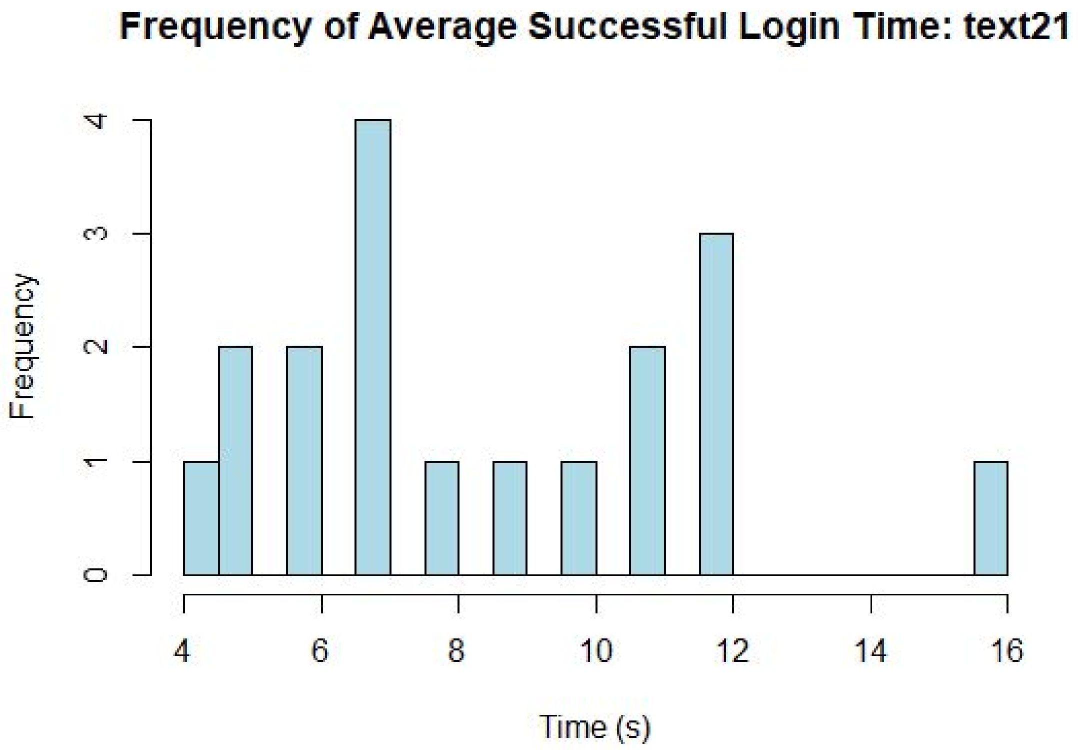
Number of Unsuccessful Logins Histogram for Image Password Scheme



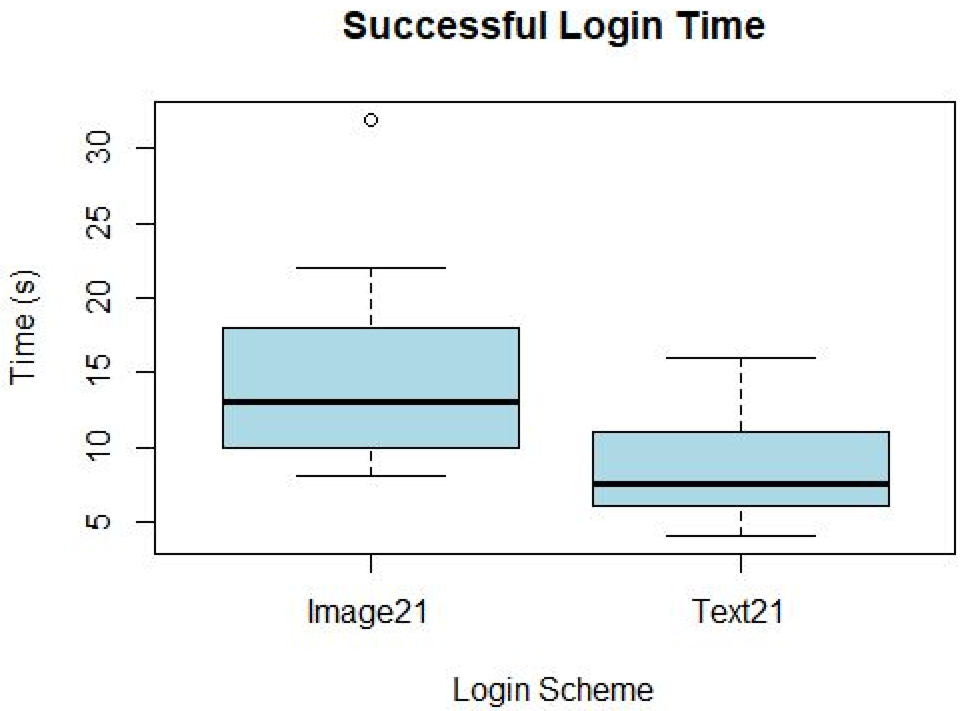
Number of Unsuccessful Logins Histogram for Text Password Scheme



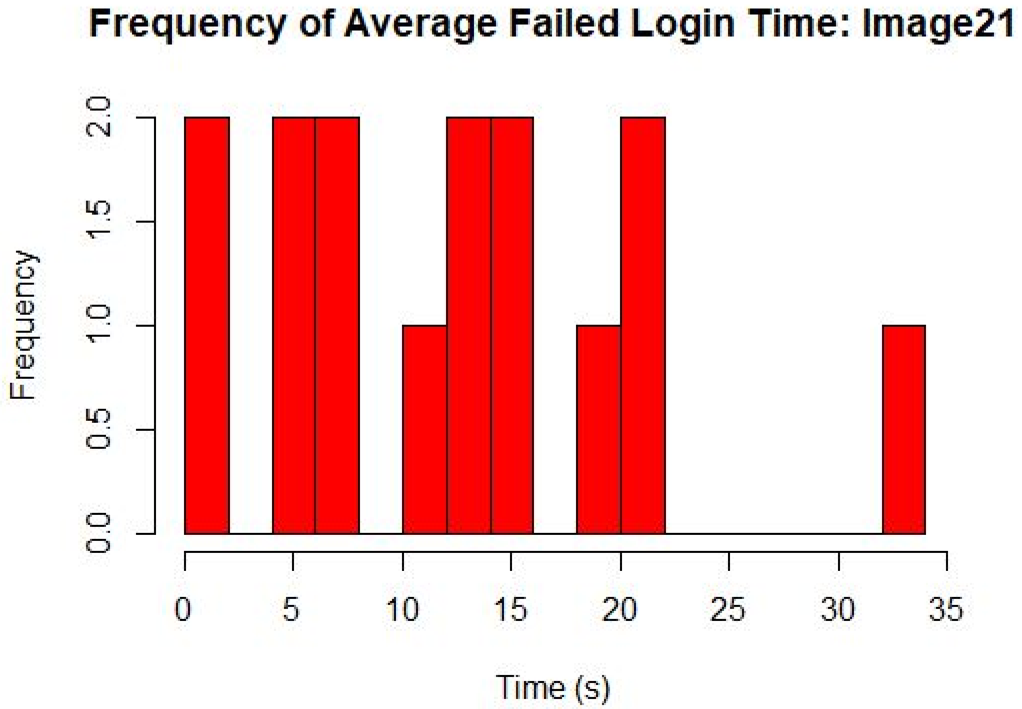
Successful Login Time Histogram Image Password Scheme



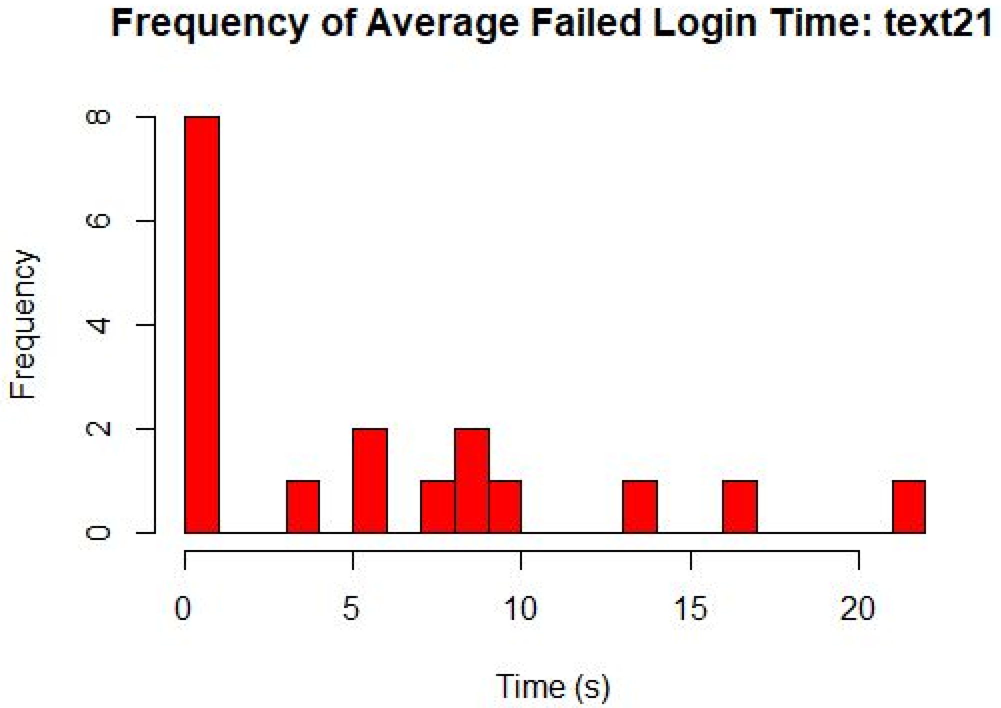
Successful Login Time Histogram Text Password Scheme



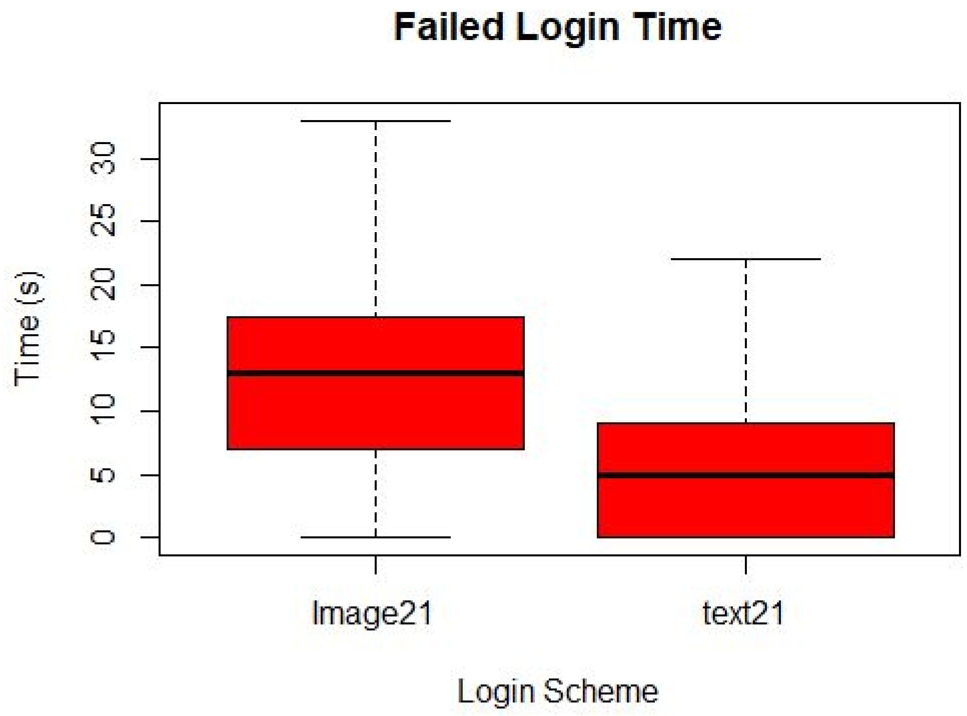
Successful Login Time per User Boxplot



Failed Login Time Histogram Image Password Scheme



Failed Login Time Histogram Text Password Scheme



Unsuccessful Login Time per User Boxplot

The above descriptive statistics show that on average, people more frequently successfully logged in using the text based scheme compared to the image based scheme (84.54% vs 79.87%). Additionally, users would press the submit button in less time while using the text based scheme which lets us conclude that they could recall their passwords quicker than when using the image based scheme.

From the histograms and boxplots, we can tell that both the average successful login time and failed login time are both shorter for the text21 password scheme than the image password scheme. This could mean that with respect to entering a password, the text21 scheme is easier to use. The difference in time could also mean that most users that used the text21 scheme had an easier time remembering their passwords than those who used the Image21 scheme.

Part 2

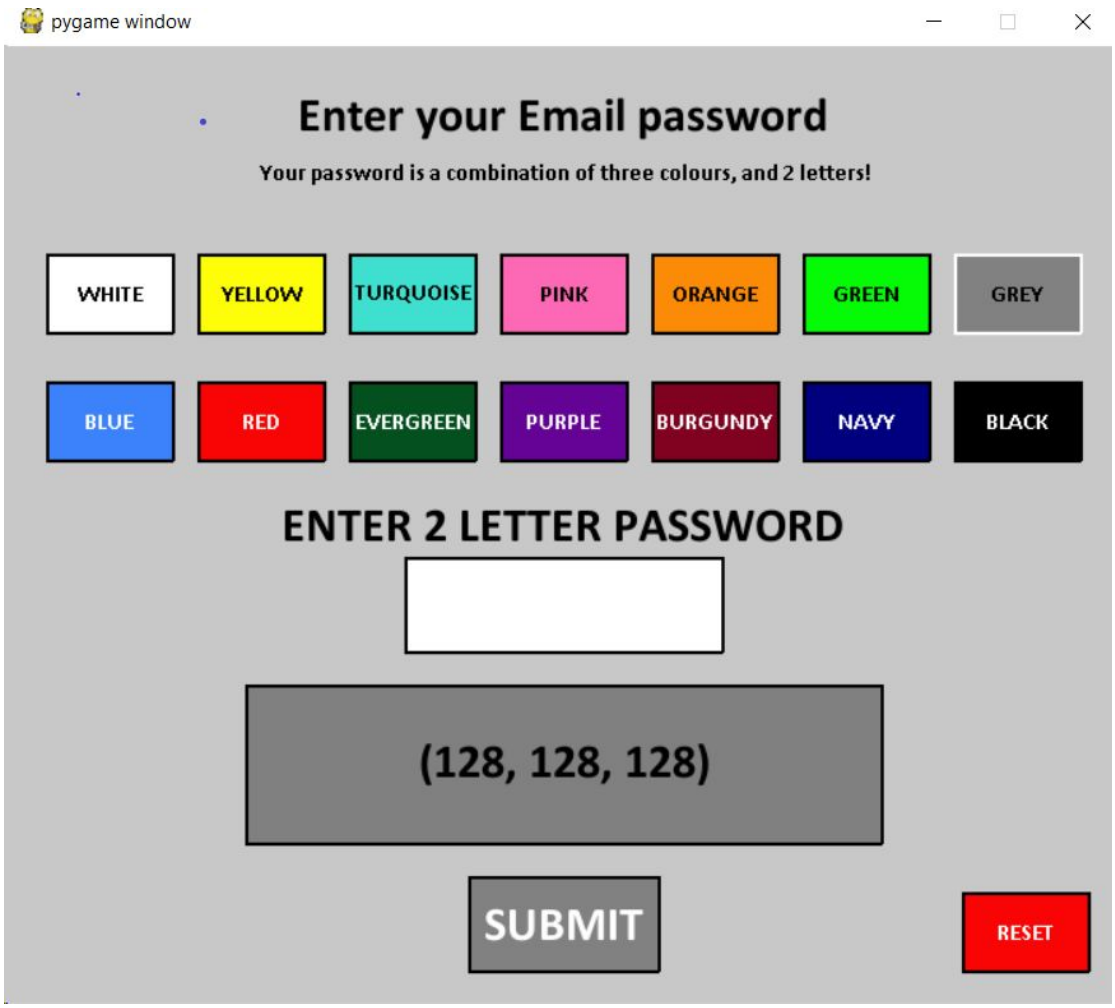
Password Scheme Design

The design of the password scheme is the colour password, using a sequence of colours followed by modification of the colour using letters. The use of colours for the password scheme was to be more visually appealing to the users rather than a purely text based password. The design also allows the user to verify that their password has been entered correctly by displaying the RGB value of their password inside a box of the colour created. This allows the user to at-a-glance compare the result of their password with what they remember it should be at any point in entering the password, whereas for text passwords, users can usually only check that the length of the password entered is correct. Since this design focuses on colours, it is obviously not as appealing to colour-blind users, however it is not impossible to use as each colour option is labeled with text and the resulting colour box also displays the colour as a RGB value to allow for verification. The colour password is designed to be naturally split into two blocks, the colour sequence and the character sequence, for ease of memorability.

Each of the three choices of colours has 14 options, since the same colour can appear multiple times in the same password, and each of the two characters can be any of the 26 lowercase letters. The password space of the colour password we have designed is

$14^3 * 26^2 = 1854944 > 2^{20}$

Password Scheme Usage



Enter your Email password

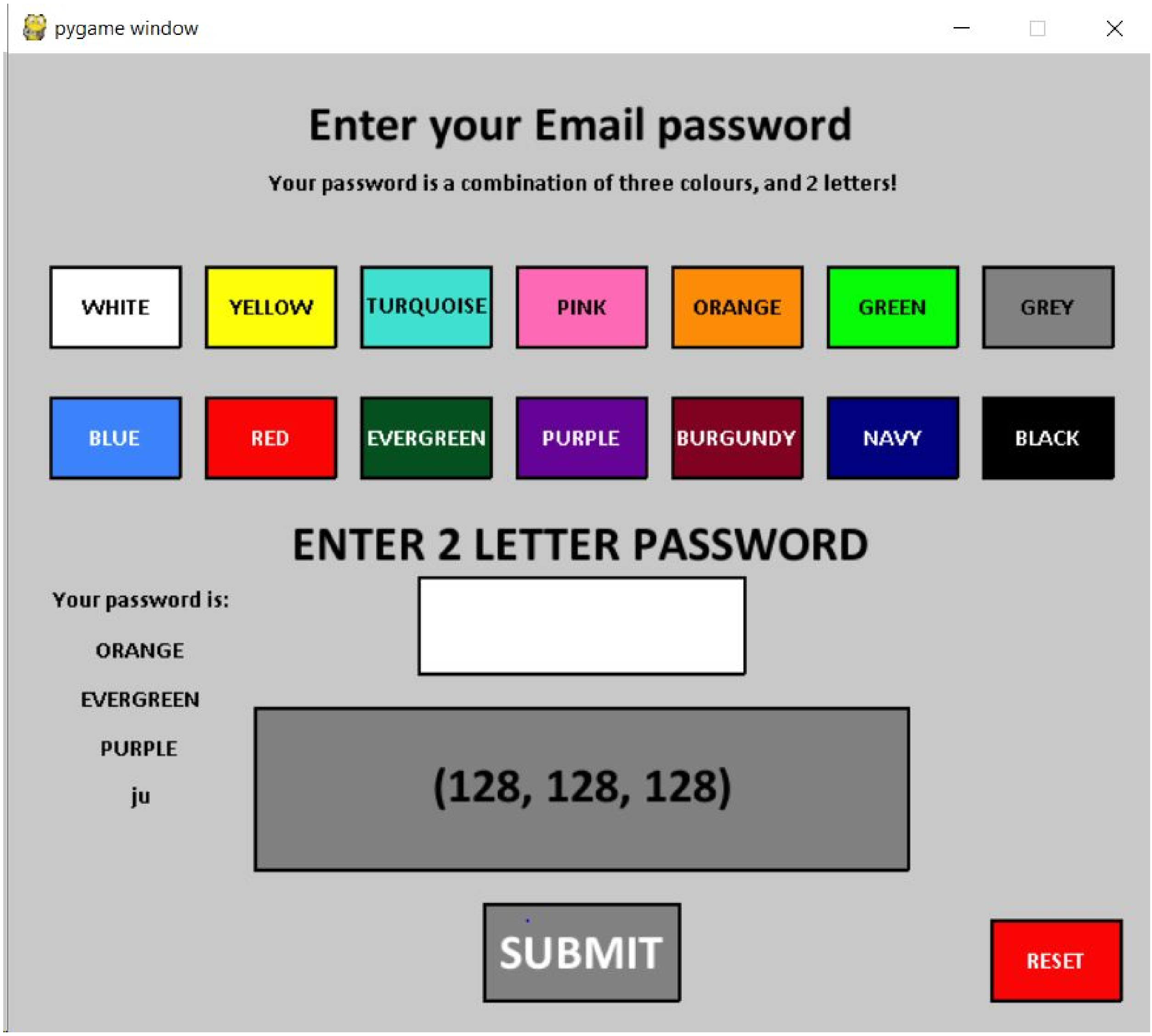
Your password is a combination of three colours, and 2 letters!

ENTER 2 LETTER PASSWORD

(128, 128, 128)

Figure 8 - New password scheme enter page

The enter page contained the 14 available colours, and the text box so that users could enter their two-letter passwords. The colour and numbers of the main grey box would change as the user entered their password, and after the password had been completely entered, they would have a final colour. This colour was used to help users verify they entered the correct password. The submit button stayed grey until the user had a valid password entered. The reset button could be used to completely reset the password, allowing users to reselect their three colours. If the user submitted an incorrect password, a message would appear and they would get another chance to enter their password. If they submitted three incorrect passwords, they would be kicked out. If they submitted the right password, they would also be kicked out, but this time a success message would be printed in the terminal.



Enter your Email password

Your password is a combination of three colours, and 2 letters!

ENTER 2 LETTER PASSWORD

Your password is:

ORANGE

EVERGREEN

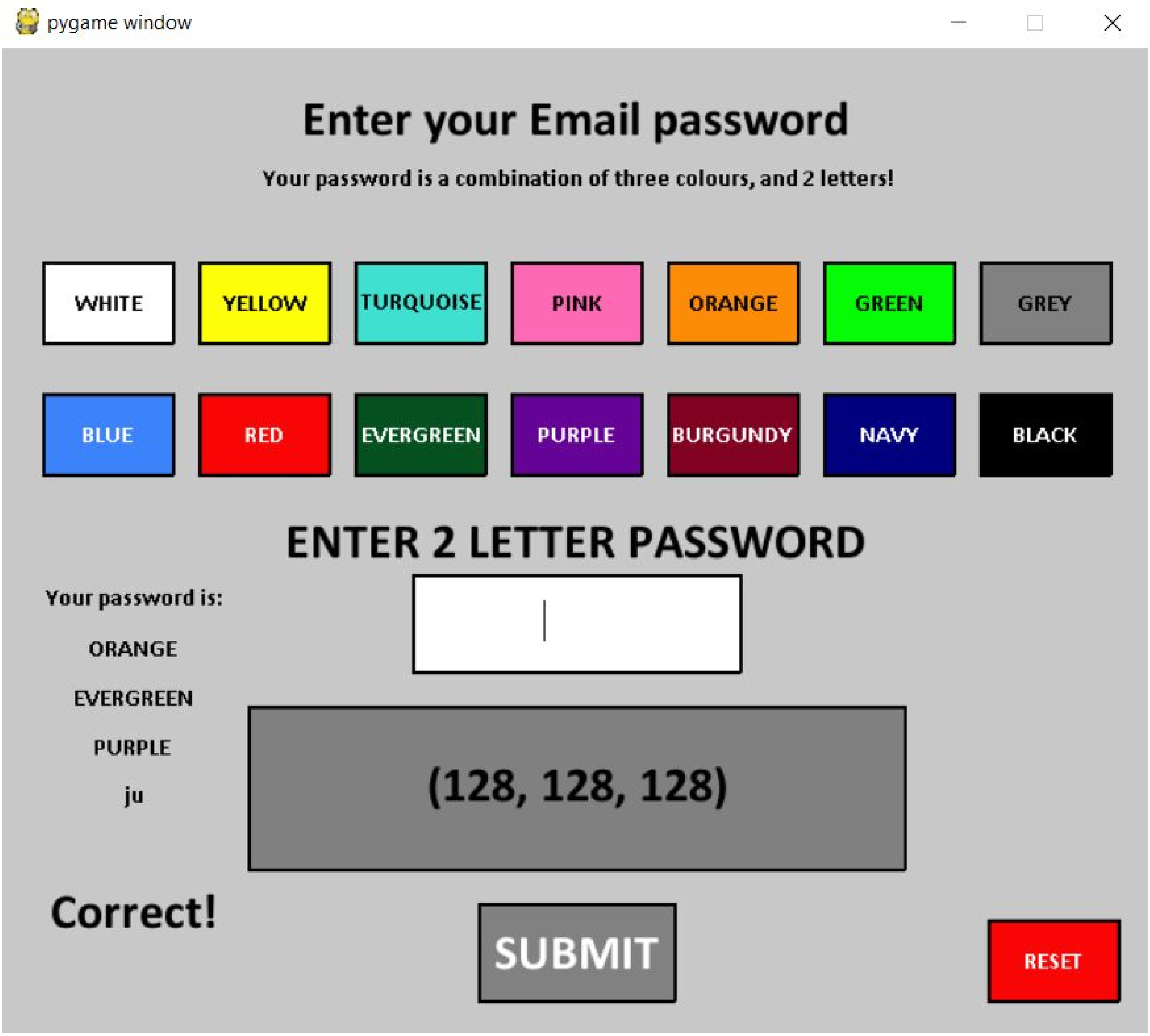
PURPLE

ju

(128, 128, 128)

Figure 9 - New password scheme learn page

The learning page is identical to the enter page except that it displays the assigned password in the order of the colours and the character modifiers at the left side of the screen.



Enter your Email password

Your password is a combination of three colours, and 2 letters!

ENTER 2 LETTER PASSWORD

Your password is:

ORANGE

EVERGREEN

PURPLE

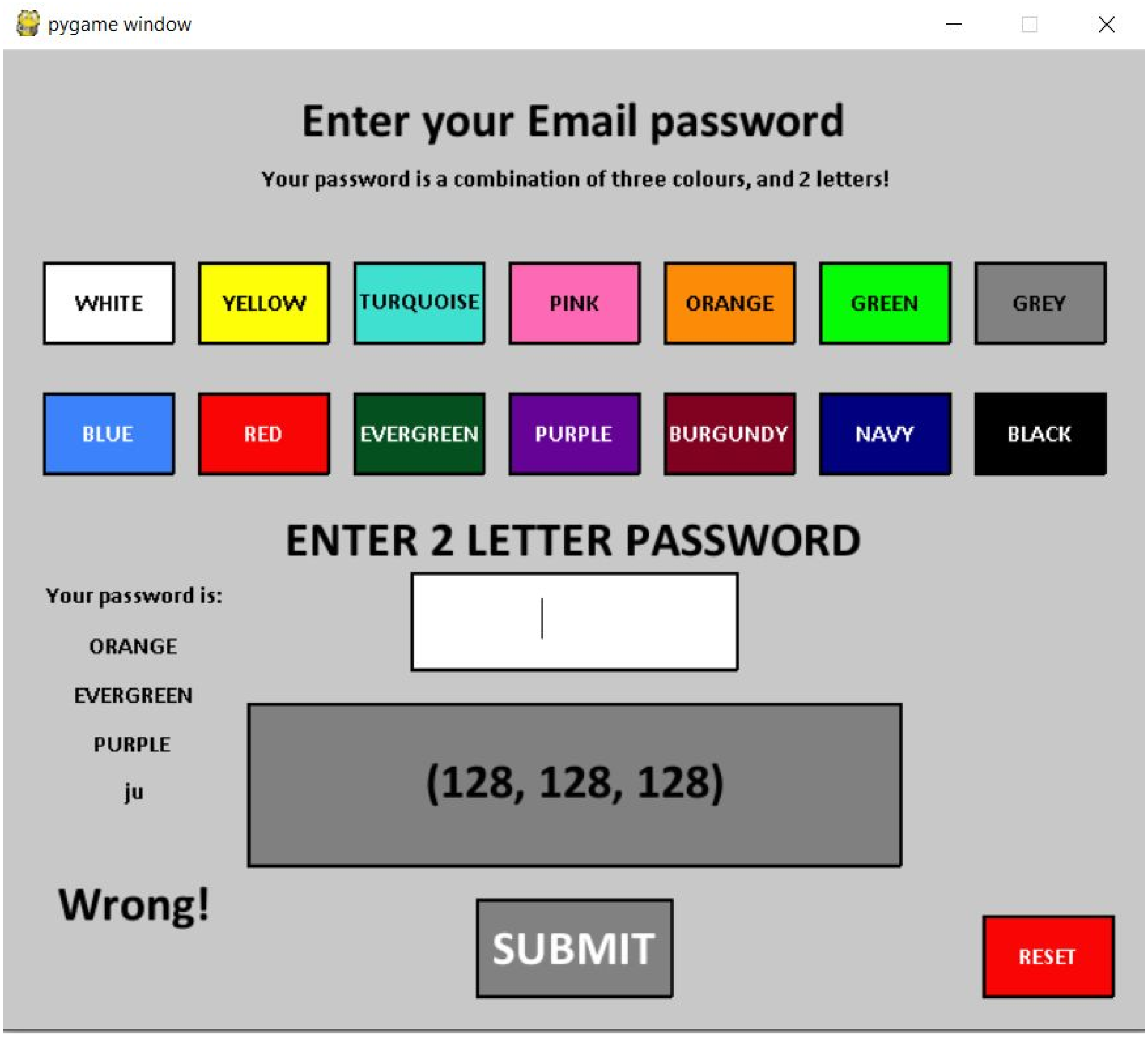
ju

(128, 128, 128)

Correct!

Figure 10 - New password scheme learn page (correct)

After pressing submit with the correct password, “Correct!” will appear for a short while in the bottom left corner of the screen.



Enter your Email password

Your password is a combination of three colours, and 2 letters!

ENTER 2 LETTER PASSWORD

Your password is:

ORANGE

EVERGREEN

PURPLE

ju

(128, 128, 128)

Wrong!

Figure 11 - New password scheme learn page (incorrect)

After pressing submit with an incorrect password, “Wrong!” will appear for a short while in the bottom left corner of the screen.

Code Information for new password authentication framework:

Code is located at:

https://github.com/JeremyDenHartogh/Comp3008Project2/tree/master/Part2

Included are 5 files related to the testing of the authentication scheme:

- PassAttempts.csv - a log file of all login attempts

- PassGenerator.py - Program used to generate new passwords for testing
- passwords.txt - text file containing all passwords for generated users
- SamplePassScheme.py - Program that runs the framework. Takes 3 input variables (learn/enter mode, user id, account type)
- pygame_textinput.py - External library, allows for text input in pygame.
  Source: https://github.com/Nearoo/pygame-text-input/blob/master/pygame_textinput.py

Documentation of the python files is stored locally in each of the python files

A readme with further information about all source is also stored at:
https://github.com/JeremyDenHartogh/Comp3008Project2/blob/master/Readme.txt

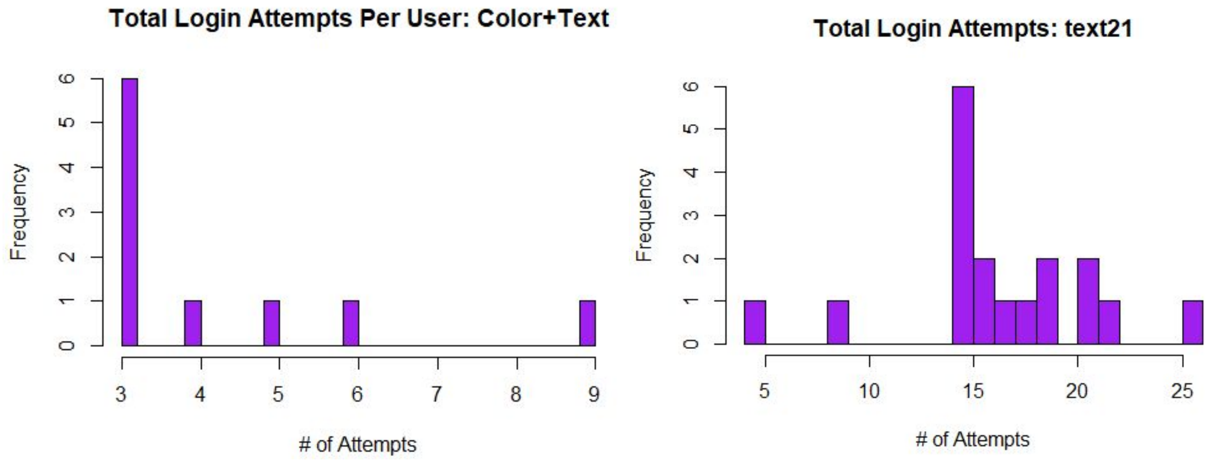
Usability Testing Results

	Colour & Text Scheme
Number of Total Login Attempts Mean	4.2
Number of Total Login Attempts Median	3
Number of Total Login Attempts Standard Deviation	1.98885785
Number of Successful Login Attempts Mean	2.3
Number of Successful Login Attempts Median	3
Number of Successful Login Attempts Standard Deviation	1.25166556

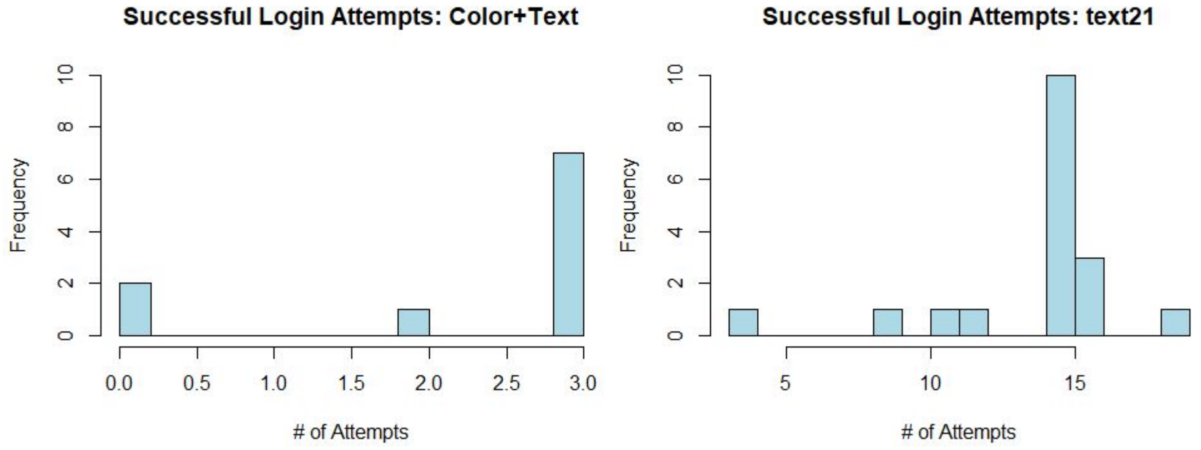
Number of Unsuccessful Login Attempts Mean	1.9
Number of Unsuccessful Login Attempts Median	0
Number of Unsuccessful Login Attempts Standard Deviation	3.17804972

Successful Login Time Mean	6.7
Successful Login Time Median	7
Successful Login Standard Deviation	4.1379007
Unsuccessful Login Time Mean	4.6
Unsuccessful Login Time Median	0
Unsuccessful Login Standard Deviation	6.2039414

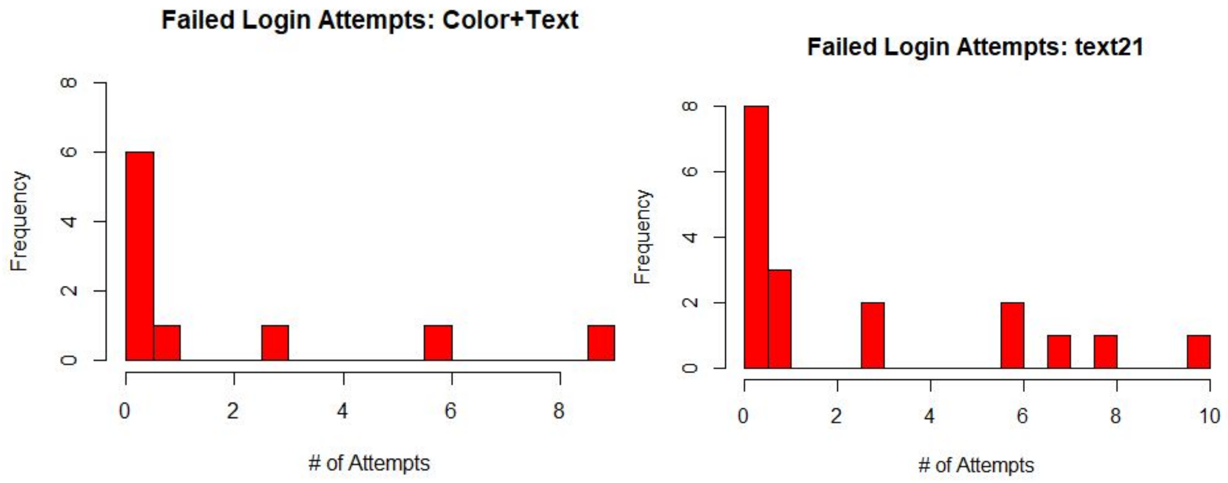
Descriptive Statistics for Colour and Text Scheme



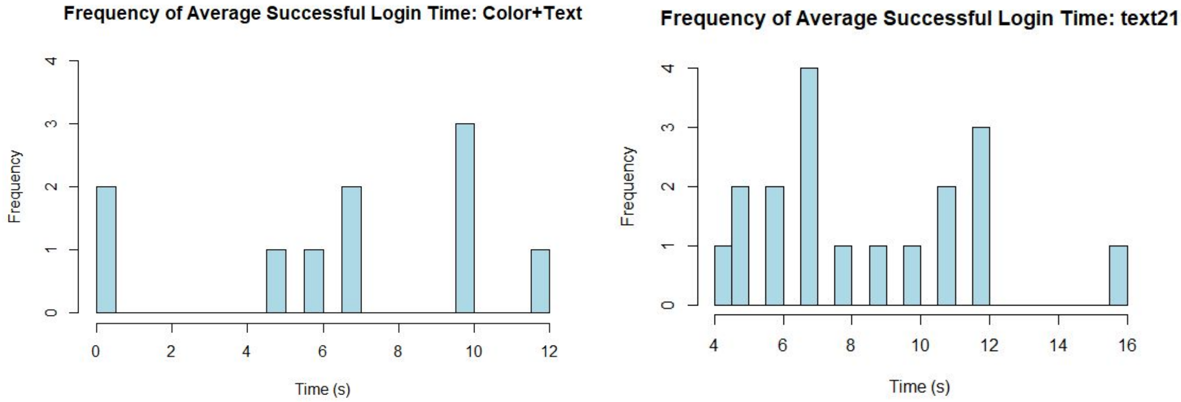
Comparison of login attempt frequencies for the color&text and text schemes



Comparison of successful login attempt frequencies for the color&text and text schemes

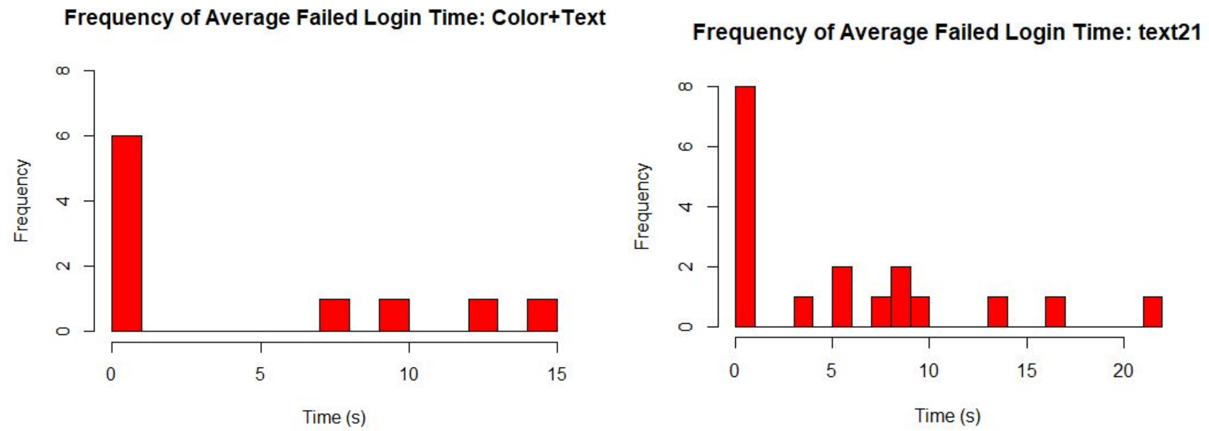


Comparison of failed login attempt frequencies for the color&text and text schemes



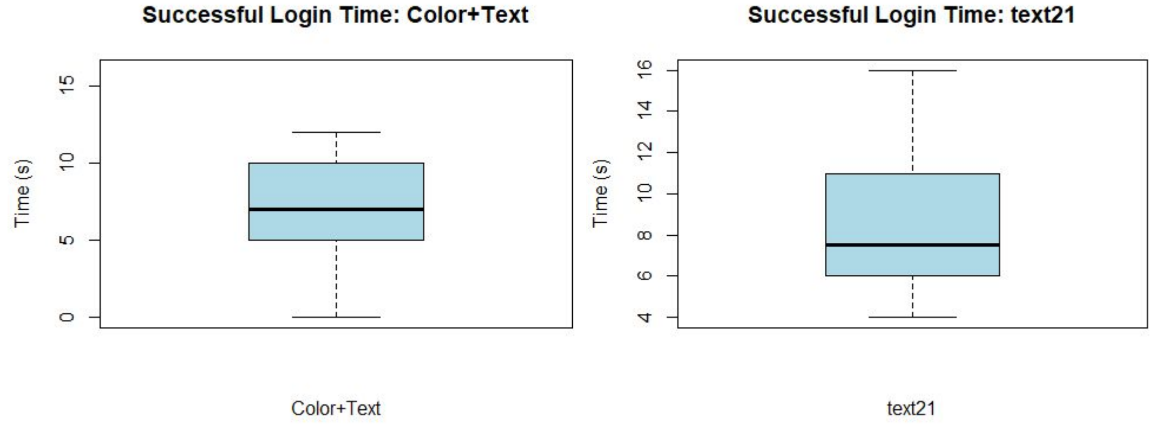
Comparison of successful login time frequencies for the color&text and text schemes

For the Color+Text scheme, the most common successful entry times were 7 and 10 seconds. As for the text21 scheme, the majority of users successfully entered their passwords between 4 and 12 seconds.



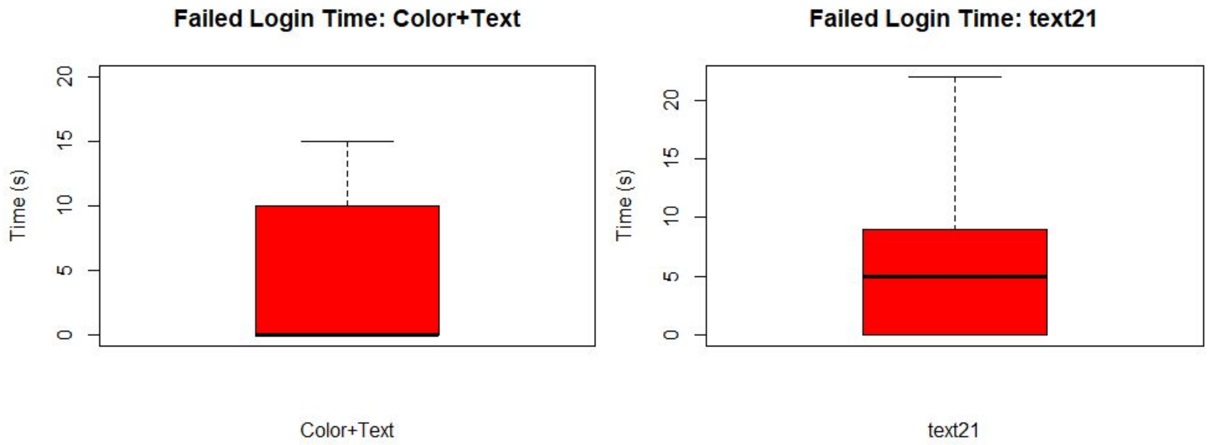
Comparison of failed login time frequencies for the color&text and text schemes

By analyzing the two histograms above, we can tell that there is very little difference between the two schemes in terms of failed login time. For the Color+Text scheme, most users did not fail a single time to enter their passwords, while those who did, did so between 6 and 15 seconds. The text21 scheme yielded similar results, with many users not failing once, and those who did fail mostly did so between 5 and 10 seconds, with a few taking longer than that.



Comparison of successful login time for the color&text and text schemes

By analyzing the two boxplots above, we can tell that there is very little difference between the two schemes in terms of successful login time. For the Color+Text scheme, the majority of users entered their passwords between 5 and 10 seconds on average, while for the text21 scheme, the average time for the majority of users is between 6 and 11 seconds.



Comparison of failed login time for the color&text and text schemes

By analyzing the two boxplots above, we can tell that there is little to no difference between the two schemes in terms of failed login time. Both schemes had the majority of users enter their passwords under 10 seconds on average.

New password scheme vs. Text21:

Hypothesis: There will be a difference in time taken to use each password scheme

```
Welch Two Sample t-test
data:  times1$SuccessTime and times2$SuccessTime
t = 1.2652, df = 15.099, p-value = 0.225
alternative hypothesis: true difference in means is not equal to 0
95 percent confidence interval:
 -1.306715  5.128937
sample estimates:
```

```
mean of x mean of y
 8.611111  6.700000
```

We recorded the time taken for successfully entering the user’s password using the colour&text password scheme and compared it to the given data for text passwords. The mean times were 8.61s (S.D. 3.20) and 6.7s (S.D. 4.14) for text and colour&text passwords respectively.

To compare the times taken to enter the passwords we used an unpaired t-test. Results show that there were no significant differences in the time taken for each scheme ($t = 1.2652$, $p \approx 0.225$).

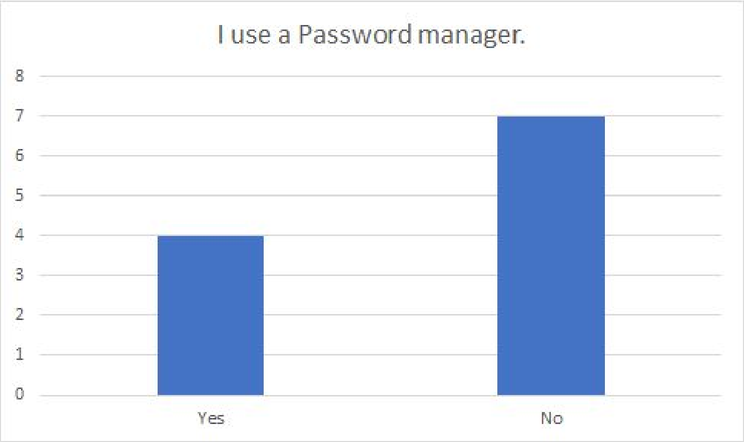
Survey results:

Pdf of survey questions located at:
https://github.com/JeremyDenHartogh/Comp3008Project2/blob/master/Part2/survey.pdf
LimeSurvey link: https://hotsoft.carleton.ca/comp3008limesurvey/index.php/772119?lang=en
The survey gathered 11 responses despite having only 10 usability testing participants. Due to the anonymity of the surveys we don’t know which responses to ignore, so all of them are included in the following statistics. The following questions have been answered using a Likert scale from 1 to 5 with 1 disagreeing with or disliking the statement and 5 agreeing with or liking the statement.

Question	**Mean**	**Median**	**StDev**
How much do you like the colours?	4.18	4	0.8739
What is your opinion on the mix of colours and text?	3	3	0.8944
What is your opinion of using text only passwords?	3.91	4	0.9439
Colour & text passwords are easy to remember.	3.27	3	1.1037
Text passwords are easy to remember.	3.55	4	0.5222
The colour & text password was difficult to input.	2.27	2	0.7862
Longer colour & text passwords would be just as easy to use.	1.82	2	0.7508
It is clear how to use colour & text passwords.	3.55	4	1.4397
I use a Password manager.	4 Yes/7 No 0.36	0	0.5045

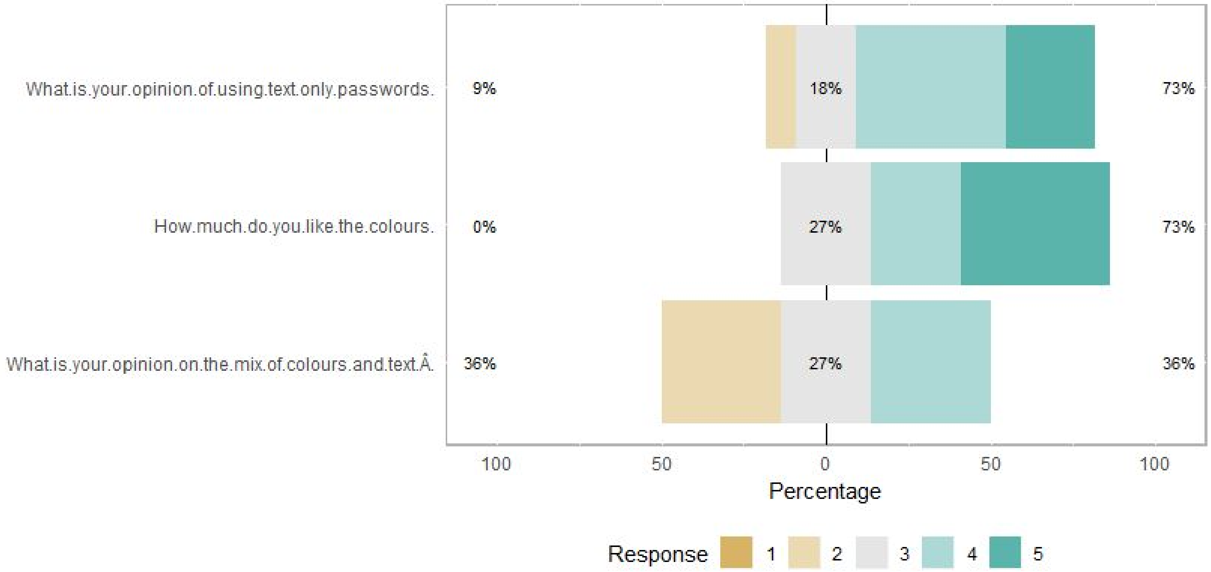
It is easy to learn how to use the colour & text password.	4.45	5	0.6876
I feel that text passwords are secure.	3.45	4	1.1282
I feel that colour & text passwords are secure.	3.55	3	1.2136
I prefer text-only passwords to colour & text passwords.	3.27	3	1.009

Descriptive statistics for survey data



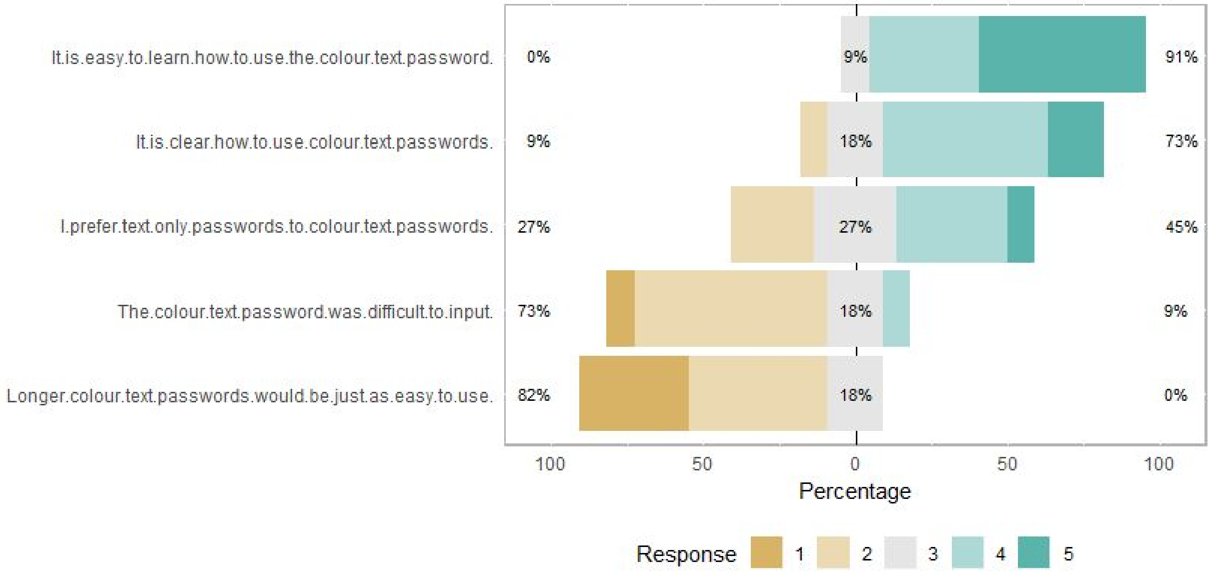
Responses to statement “I use a Password manager”

Most participants do not use a password manager, so remembering their passwords is important for them to access their accounts.



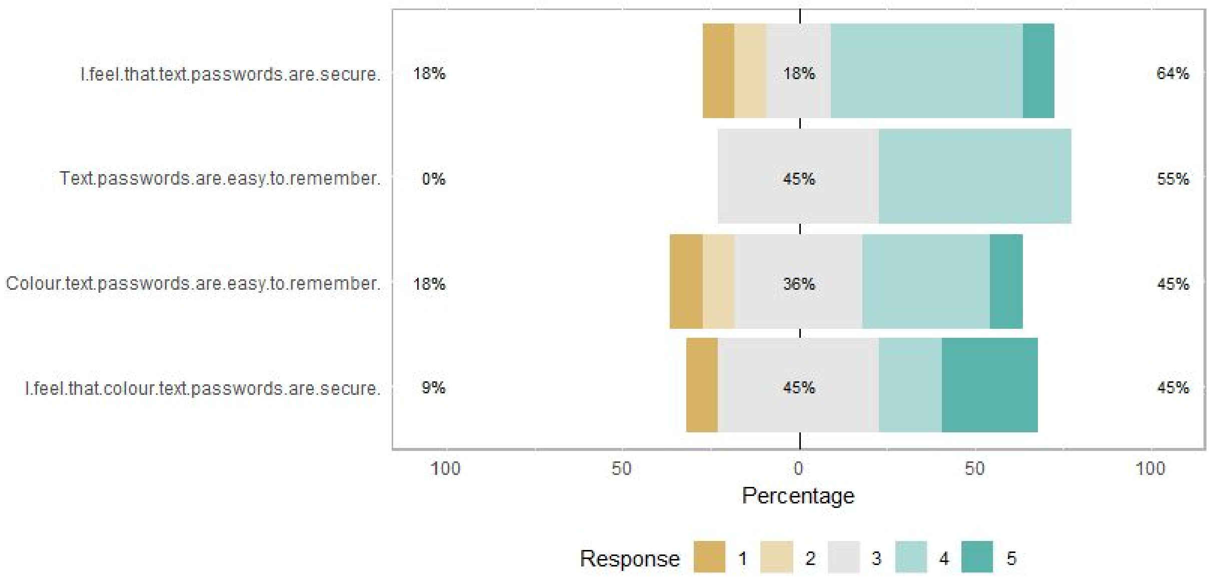
Responses to the use of colour in the password scheme (1: strongly dislike - 5: strongly like)

Users generally enjoyed the use of colours in the new scheme.



Responses to agree/disagree questions (1: strongly disagree - 5: strongly agree)

We can see that users found it easy to learn and use the colour&text passwords, however they expect longer passwords to be much more difficult to use.



Responses to questions directly comparing text only to colour and text passwords (1: strongly disagree - 5: strongly agree)

We can see that while both password schemes were viewed mostly favourably, the text only password scheme was slightly prefered by our participants.

Inferential Statistics

Code is located at:

https://github.com/JeremyDenHartogh/Comp3008Project2/blob/master/Part2/3008part2script.R

Hypothesis: There will be a difference in users' perceptions of memorability between the two password schemes

```
Wilcoxon signed rank test with continuity correction
data:  tab$Colour.text.passwords.are.easy.to.remember. and
tab$Text.passwords.are.easy.to.remember.
V = 9, p-value = 0.429
alternative hypothesis: true location shift is not equal to 0
```

Users responded to a 5 point Likert scale question assessing the memorability of text based passwords and text&colour passwords, with 1 = not very memorable and 5 = very memorable. The mean responses were 3.55 (S.D. 0.522) and 3.27 (S.D. 1.10) for the text and colour&text schemes respectively.

To compare perceptions of the schemes we used a related samples Wilcoxon test. Results show that there were no significant differences in memorability between the two schemes(p ≈ 0.43).

Hypothesis: There will be a difference in users' perceptions of security between the two password schemes

```
Wilcoxon signed rank test with continuity correction
data:  tab$I.feel.that.text.passwords.are.secure. and
tab$I.feel.that.colour.text.passwords.are.secure.
V = 6, p-value = 0.7656
alternative hypothesis: true location shift is not equal to 0
```

Users responded to a 5 point Likert scale question assessing the how secure they feel text based passwords and text&colour passwords are, with 1 = not very secure and 5 = very secure. The mean responses were 3.45 (S.D. 1.13) and 3.55 (S.D. 1.21) for the text and colour&text schemes respectively.

To compare the perceived security of the schemes we used a related samples Wilcoxon test. Results show that there were no significant differences in perception of security between the schemes (p ≈ 0.77).

We find from the inferential statistics that there are no statistically significant differences between user perception or usability between colour&text and text-only passwords.

Workload Distribution and Summary

Esti

- Worked on pseudo code for data cleaning/formatting (Part 1)
- Worked on data cleaning and formatting code (Part 1)
- Wrote explanation of data cleaning process (Part 1)
- Calculated half of the descriptive statistics (Part 1)
- Tested authentication scheme with 2 participants (Part 2)
- Helped adjust part 1 code to parse part 2 csv (Part 2)
- Calculated and wrote descriptive statistics (Part 2)
- Commented csv parsers

Jordan

- Designed new authentication scheme (Part 2)
- Implemented new authentication scheme (Part 2)
- Implemented testing framework (Part 2)
- Tested authentication scheme with 3 participants (Part 2)
- Calculated descriptive and inferential statistics for survey results (Part 2)

Shaan

- Worked on pseudo code for data cleaning/formatting (Part 1)
- Worked on data cleaning and formatting code (Part 1)
- Wrote explanation of data cleaning process (Part 1)
- Created histograms and boxplots (Part 1)
- Tested authentication scheme with 2 participants (Part 2)
- Created Graphs to compare usability of text21 and our password scheme (Part 2)

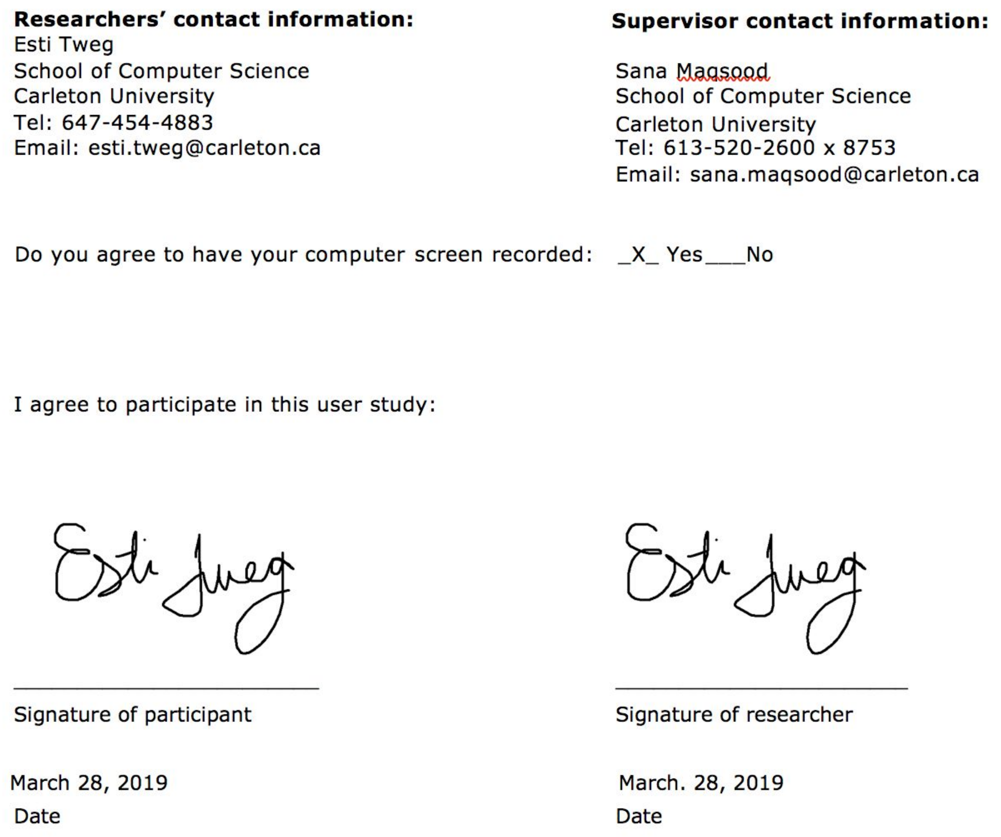
Jeremy

- Designed new authentication scheme (Part 2)

- Implemented new authentication scheme (Part 2)
- Implemented testing framework (Part 2)
- Created logger for authentication scheme testing (Part 2)
- Tested authentication scheme with 3 participants (Part 2)
- Wrote documentation in the report for the new password scheme (Part 2)
- Wrote documentation for source code in files in part 2 related to the new password scheme (Part 2)

Appendix

Signed Consent Forms



Researchers' contact information:
Esti Tweg
School of Computer Science
Carleton University
Tel: 647-454-4883
Email: esti.tweg@carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: _X_ Yes___No

I agree to participate in this user study:

Esti Tweg
____
Signature of participant

March 28, 2019
Date

Esti Tweg
____
Signature of researcher

March. 28, 2019
Date

Researchers' contact information:
Esti Tweg
School of Computer Science
Carleton University
Tel: 647-454-4883
Email: esti.tweg@carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: _X_ Yes ___No

I agree to participate in this user study:

Signature of participant

Esti Tweg

Signature of researcher

April 2, 2019
Date

April 2, 2019
Date

Researchers' contact information:

Jordan Li
School of Computer
Science
Carleton University
Tel: 613-899-6875
Email: jordanli@cmail.carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: _✓_Yes___No

I agree to participate in this user study:

____
Signature of participant

____
Signature of researcher

MAR 29/19
Date

Mar 29/19
Date

Researchers' contact information:
Jordan Li
School of Computer
Science
Carleton University
Tel: 613-899-6875
Email: jordanli@cmail.carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ✓ Yes___No

I agree to participate in this user study:

Signature of participant

Signature of researcher

29/03/19
Date

Mar 29/19
Date

Researchers' contact information:
Jordan Li
School of Computer
Science
Carleton University
Tel: 613-899-6875
Email: jordanli@cmail.carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ✓ Yes___No

I agree to participate in this user study:

Signature of participant

Signature of researcher

Apr 4/19
Date

Apr 4/19
Date

Researchers' contact information:

Shaan Malik
School of Computer
Science
Carleton University
Tel: 819-665-7918
Email: shaan.malik@carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: _✓_Yes___No

I agree to participate in this user study:

Signature of participant

Signature of researcher

2019/04/02

Date

2019/04/02

Date

Researchers' contact information:

Shaan Malik
School of Computer
Science
Carleton University
Tel: 819-665-7918
Email: shaan.malik@carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ___[✓ Yes]___No

I agree to participate in this user study:

____

Signature of participant

____

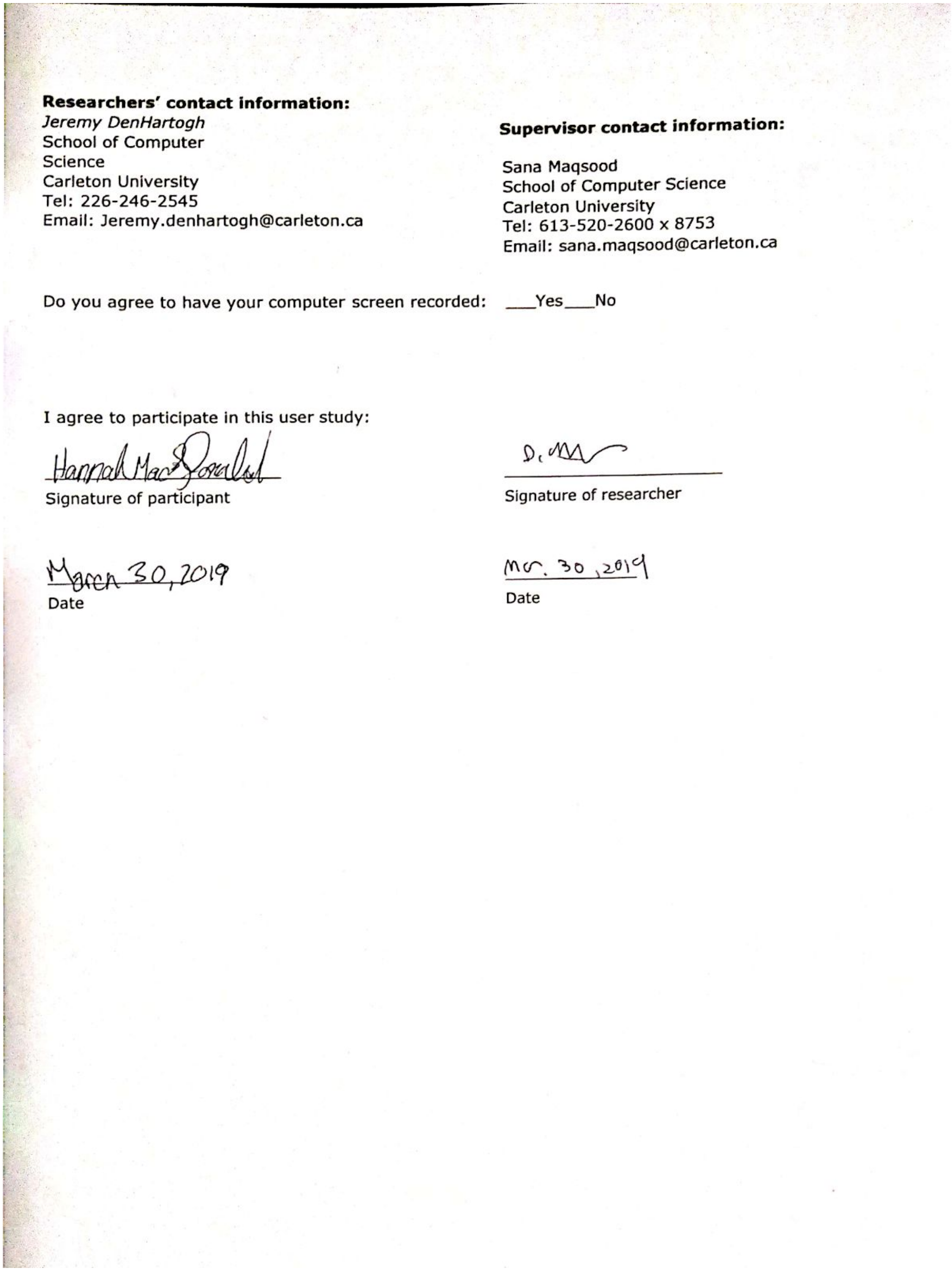
Signature of researcher

2019/04/02

Date

2019/04/02

Date



Researchers' contact information:
Jeremy DenHartogh
School of Computer
Science
Carleton University
Tel: 226-246-2545
Email: Jeremy.denhartogh@carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ___Yes___No

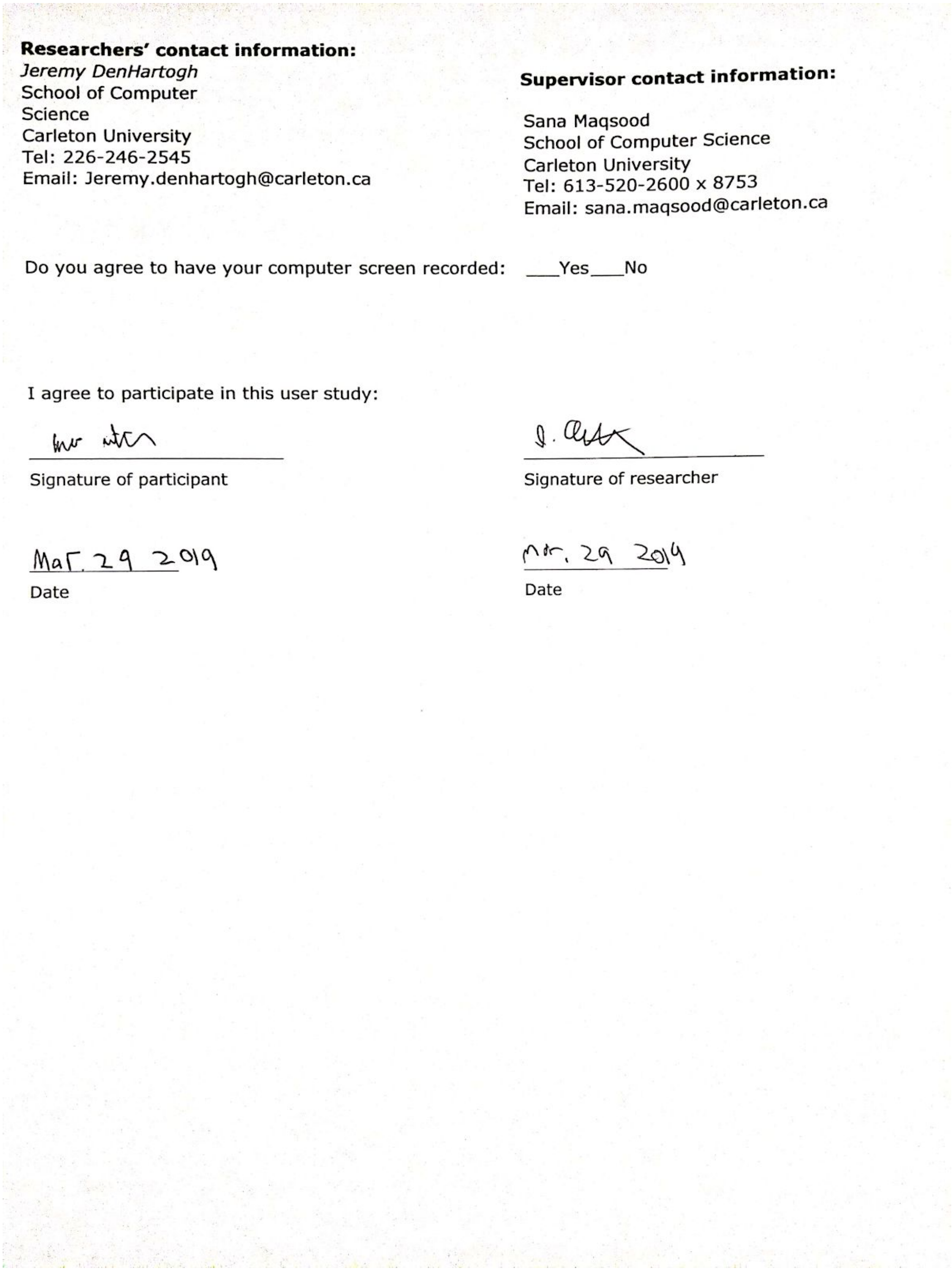
I agree to participate in this user study:

Hannah MacDonald
Signature of participant

Signature of researcher

March 30, 2019
Date

Mar. 30, 2019
Date



Researchers' contact information:
Jeremy DenHartogh
School of Computer Science
Carleton University
Tel: 226-246-2545
Email: Jeremy.denhartogh@carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ___Yes___No

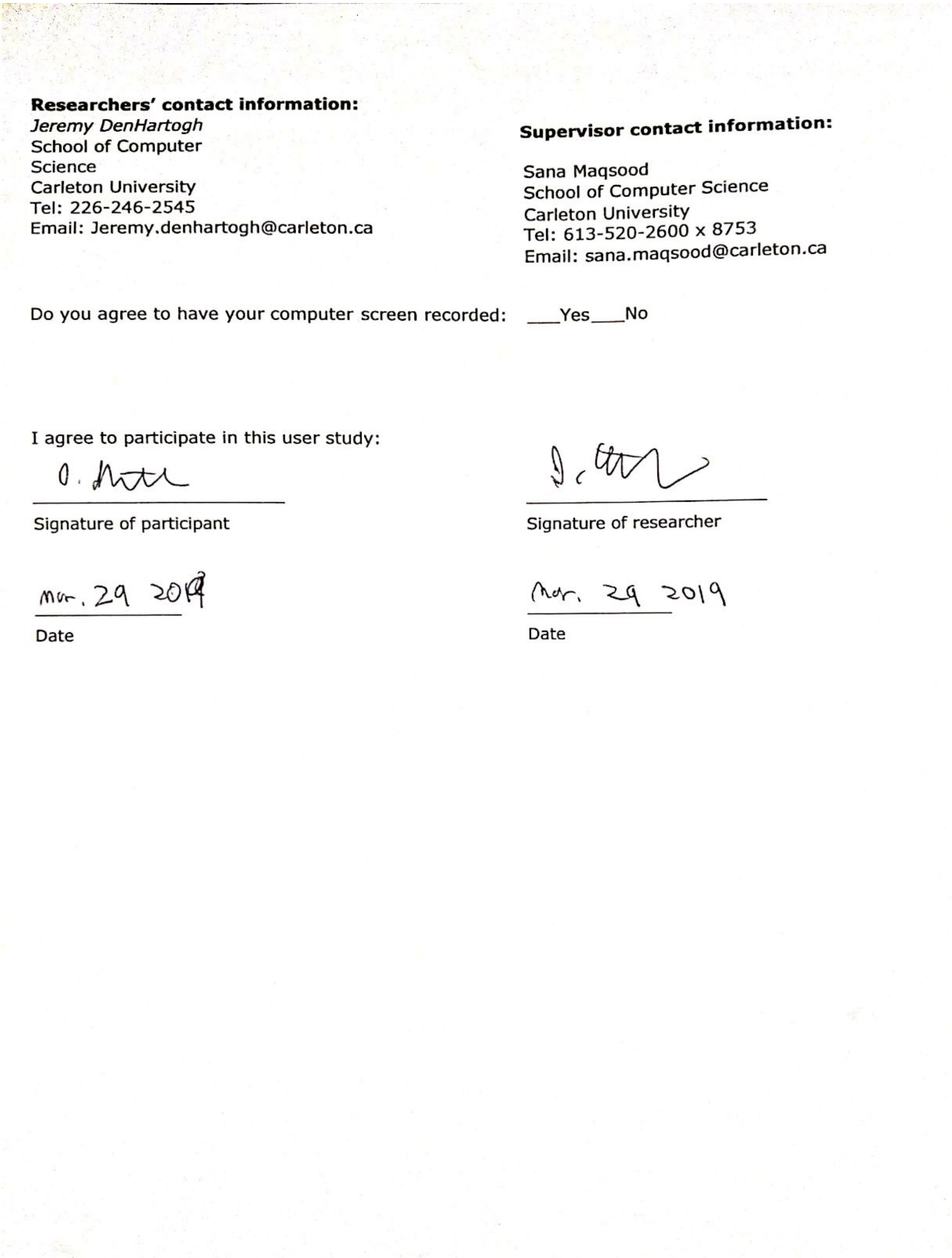
I agree to participate in this user study:

____
Signature of participant

____
Signature of researcher

Mar. 29 2019
Date

Mar. 29 2019
Date



Researchers' contact information:
Jeremy DenHartogh
School of Computer
Science
Carleton University
Tel: 226-246-2545
Email: Jeremy.denhartogh@carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ___Yes___No

I agree to participate in this user study:

Signature of participant

Signature of researcher

Mar. 29 2019

Date

Mar. 29 2019

Date