# Project #2

## Quantitative Usability Evaluation

Ethan Leider, 101078035

Anant Ojha, 101072523

Zhiyu Ma, 101081611

**COMP 3008**

**Team 3008**

Dr. Sana Maqsood

# Table of Contents

**PART A**

**PART B**

# Text-based vs Image-based Passwords

Despite decades of research into alternatives, text-based passwords continue to be widely used today because of their comparative advantages. The creation and usage of passwords is key to how systems protect digital information. Password schemes are methods of authentication which applications rely on to grant users access to information. Every scheme however, has its trade-offs in terms of the usability it provides in comparison to its security. Text-based passwords can be found to contain any combinations of numbers, letters and/or special characters.  The biggest advantage text passwords have is familiarity with users. People today have already used the scheme and know the sequence of steps involved. First, a combination of characters is selected (a password) and then later used to sign-in, with the help of a physical or virtual keyboard.

Image-based passwords work similarly but do not require a keyboard. This means that unlike text passwords, they are not vulnerable to keylogger attacks. Since image-based passwords are less common, they may be more frustrating to use at first, due to the additional time and effort they require from the user. As a result, image passwords pose a steeper learning curve in comparison to text passwords. It is important to note however, that the same functionality is accomplished by both schemes at the end but, in different ways.

Consider entering a text password, the first requirement is that a keyboard must be present. Then during entry, every character selected must be concealed with a symbol (usually '•') for protection. It is often overlooked that due to this security feature it is impossible to find where typos occur during entry, as passwords appear as a sequence of symbols ('••••••••') on screen. This highlights an instance where a direct trade-off is made between usability (able to find typo) and security (hide password) features of a scheme. Since it is more important to safeguard the password in this case, usability is compromised. A drawback of text-based passwords however, is during creation/entry, the password length is always revealed!

Image passwords offer even fewer security features during creation/entry, they are extremely vulnerable to theft primarily by people in close proximity to the user. Stealing someone's password may be as simple as looking at their screen at the right time. This is the biggest pitfall of image-based password and a reason as to why they are not used for authentication today by applications. Nevertheless, image-based schemes do play a key role in detecting computer bots.

*Schemes:*

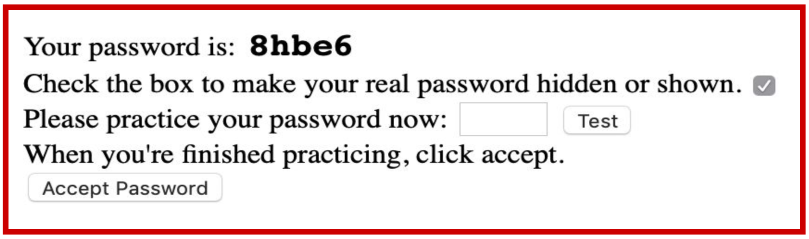
**User: svp977047**

**Scheme: textrandom; Condition: az09-5**

**User: svp123088**

**Scheme: passtiles; Condition: ImagePasstiles_Poll**

*Creation:*

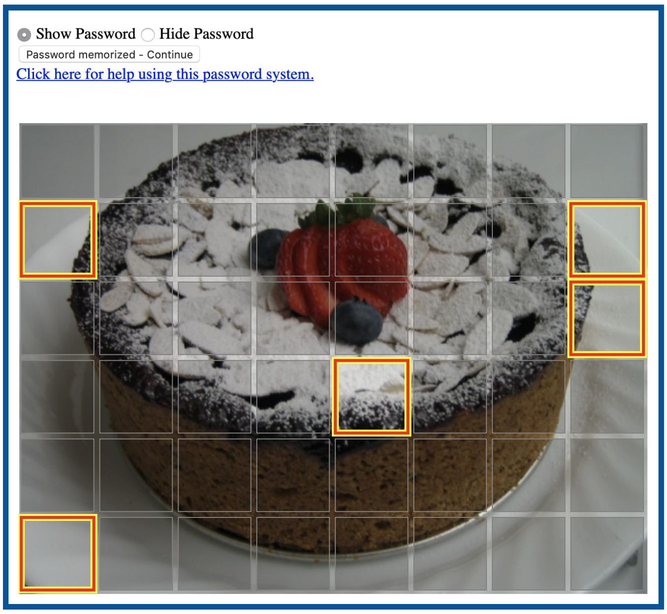


Your password is: **8hbe6**

Check the box to make your real password hidden or shown. ☑

Please practice your password now:

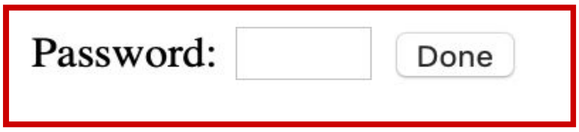
When you're finished practicing, click accept.



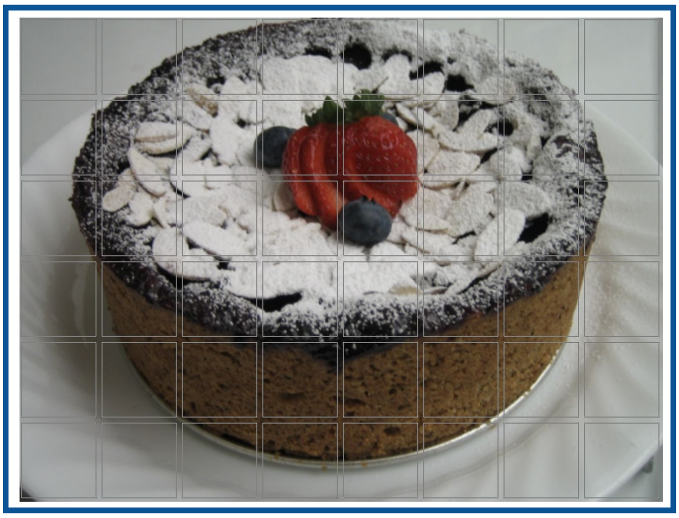
● Show Password ○ Hide Password

Click here for help using this password system.

*Entry:*



Password:

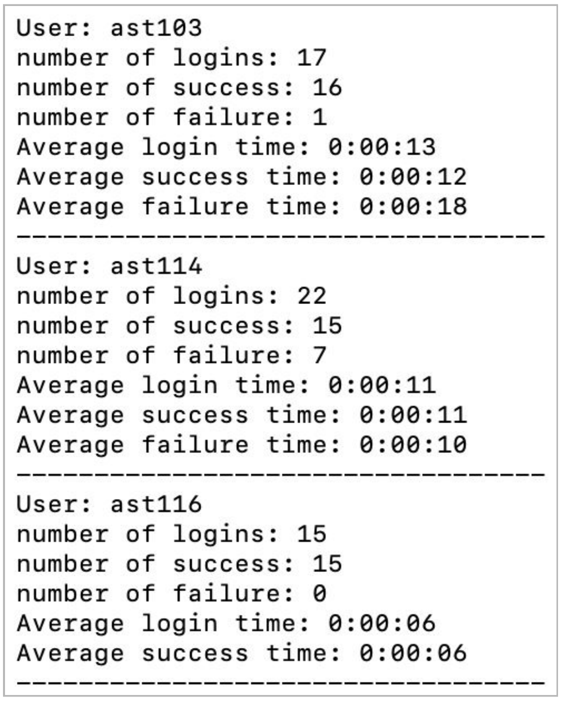


## Datalog Software

As part of this project, a datalog program was implemented to analyze and produce statistics for the provided datasets. The program, written in Python, reads CSV files containing user interaction data, then stores it into a suitable format to be analyzed later on. The analysis consists of finding the average login attempt/success/failure times of all users. To compute statistics (Mean, Median, S.D.) the NumPy library is imported and for generating graphs, MATLAB is used. After calculations are completed, the program outputs results to a new file.

When analyzing raw interactional data, it is crucial to correctly match the start and end timestamps associated with each log. This determines the amount of time spent by users on a specific task. In this case, examining the login times for each scheme. The datalog software's timestamp matching algorithm uses backtracking to solve this problem efficiently. While looping through the data, whenever a 'success' or 'failure' login is detected, the data is 'backtracked' to find the corresponding start event. Once both the start and end events are matched, their difference equals the time spent to log-in. This process is repeated for all users in both password schemes, followed by the sorting of 'successful' and 'failed' attempts and then finally computing statistics .

The final step before calculations and graphing requires removal of all outliers in both datasets. Outliers and other anomalies cause the overall statistics and shape of the data to be distorted. Removing them allows for a much stronger correlation between the data.

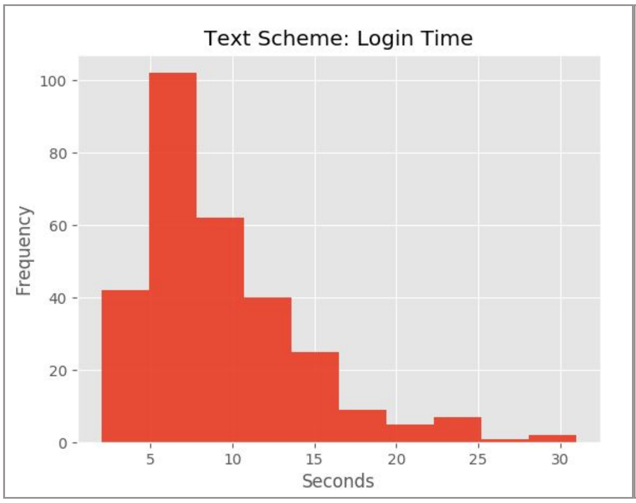


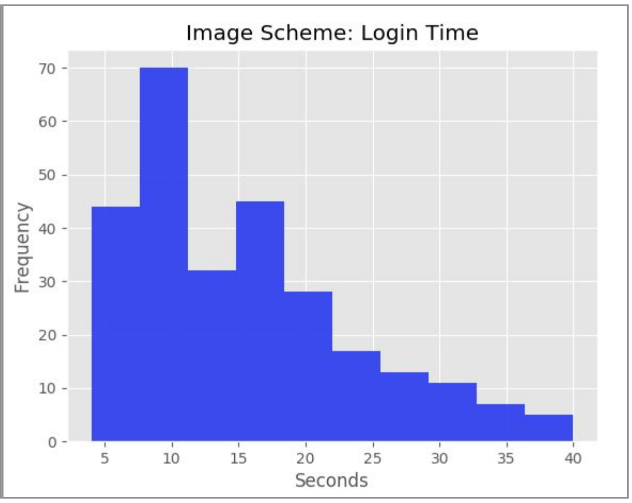
```
User: ast103
number of logins: 17
number of success: 16
number of failure: 1
Average login time: 0:00:13
Average success time: 0:00:12
Average failure time: 0:00:18
-----------------------------------
User: ast114
number of logins: 22
number of success: 15
number of failure: 7
Average login time: 0:00:11
Average success time: 0:00:11
Average failure time: 0:00:10
-----------------------------------
User: ast116
number of logins: 15
number of success: 15
number of failure: 0
Average login time: 0:00:06
Average success time: 0:00:06
-----------------------------------
```

## Descriptive Statistics

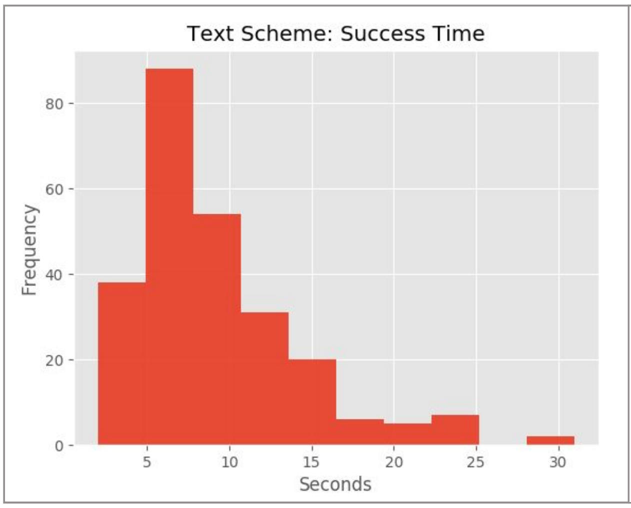
| | Text-Based | Image-Based |
|---|---|---|
| Mean # of Attempts: | **17** | **19** |
| Mean # of Successes: | **14** | **15** |
| Mean # of Failures: | **3** | **4** |
| Mean Login Time: | **10s** | **18s** |
| Mean Successes Time: | **10s** | **17s** |
| Mean Failures Time: | **12s** | **12s** |

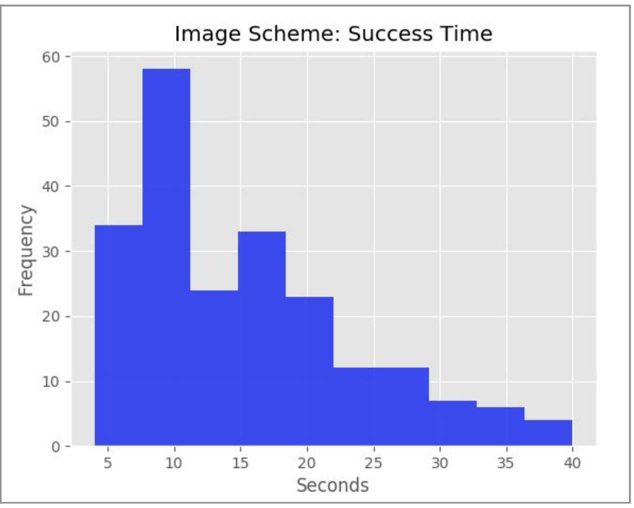
The averages computed above show that users overall took fewer attempts and also less time when using text-based passwords in comparison to image-based passwords.



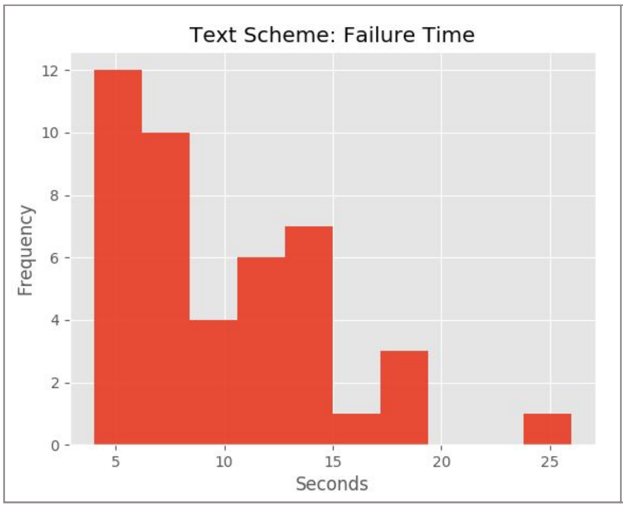


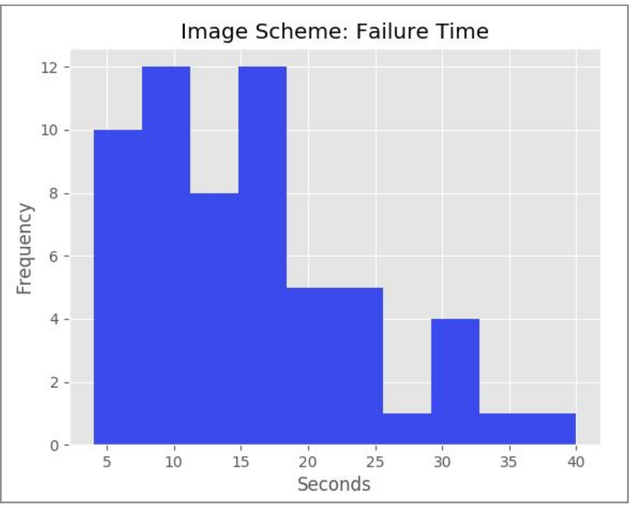
The majority of login attempt times for text passwords occur during the 7.5 second mark. Meaning that during testing, users were able to enter their text password in approximately 7.5 seconds on most attempts. For image passwords however, most users took close to 10 seconds for password entry. Seeing this, it is safe to conclude that users found it much easier to submit text passwords in comparison to image passwords since it took less time. To confirm this, the 'Mean Login Time' for both schemes can be used, text passwords on average took about 10 seconds to enter compared to 18 seconds taken by image passwords. In terms of usability, the stats indicate text-based passwords as being more user-friendly than image-based passwords, due to the minimal overall effort they require from users.



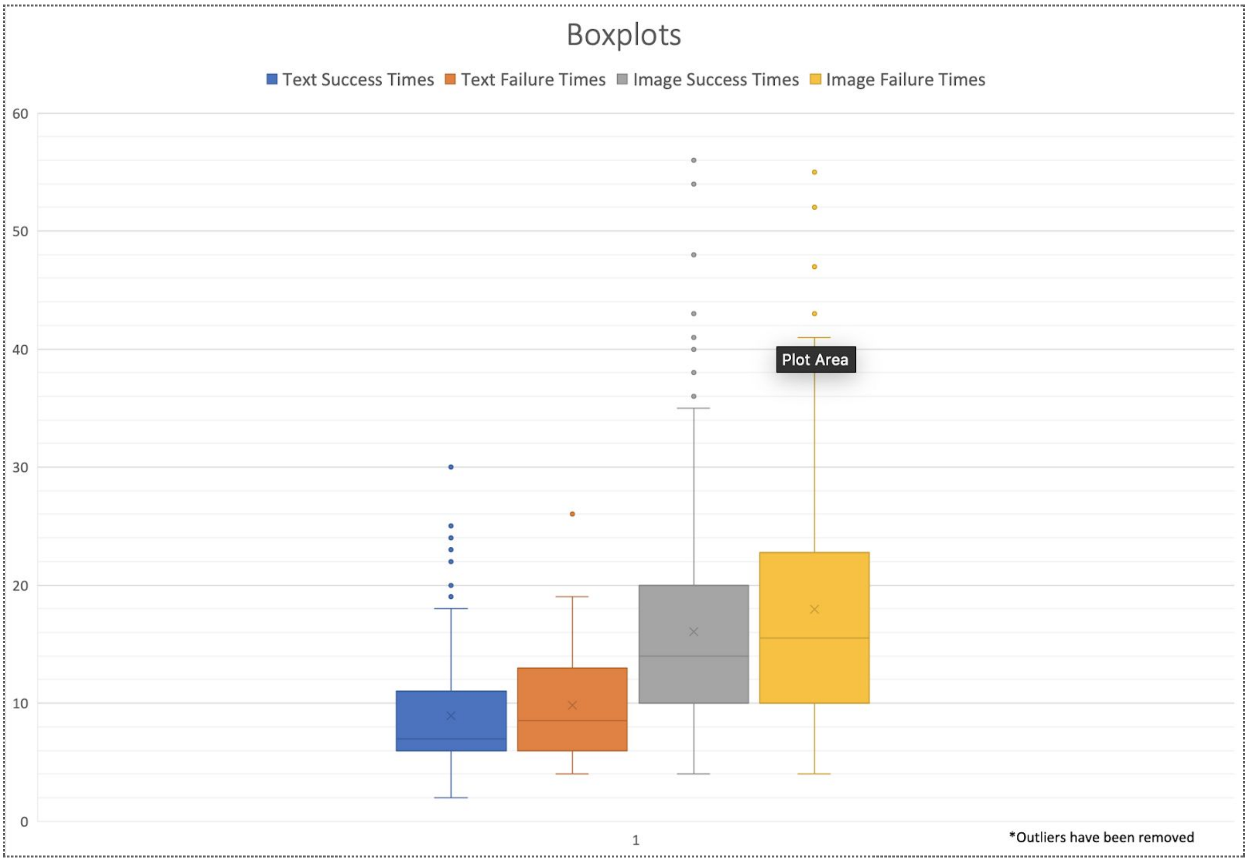


The majority of success times of users in both schemes roughly occur at the same. Most users who logged-in successfully, were able to do so in just under 10 seconds using either text or image passwords. This emphasizes the fact that users are capable of memorizing both kinds of passwords. If a user still remembers their password at entry, then it would likely take the same amount of time regardless of the scheme. The averages however differ slightly, 'Mean Successes Time' for text-based passwords is 10 seconds compared to 17 seconds for image-based passwords.





Failure times of users vary between both schemes. By looking at the histograms above, it is obvious that the entry time of text passwords is faster than that of image passwords for failed attempts. The majority of failed log-ins occur at around 5 seconds for text passwords and between 10 to 15 seconds for image passwords. The 'Mean Failures Time' of both schemes however, contradicts this and shows that on average text and image passwords take the same amount of time (12 seconds) for failed attempts. This may be caused as a result of not having enough failure data, which then creates inconsistent values.



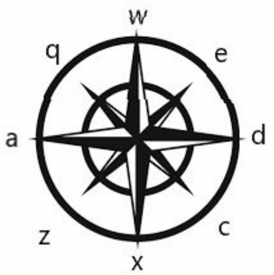
The boxplot above illustrates success and failure times for both schemes. As shown, text-based passwords are much faster than image-based passwords, sometimes requiring as little as half the time needed for entry. It is also clear that failures in either scheme tend to take longer than successes, which makes sense; entering a memorized password is easier than trying to enter a somewhat forgotten one.

In conclusion, after closely examining both schemes and their test data, text-based passwords appear to come out ahead, they are faster to use and more accurate than image-based passwords. So, when deciding which scheme to use for an application, it is important to keep in mind what users will be most comfortable with. According to the test data, text passwords offer more of an advantage.

** NOTE: all anomalies in the data were removed before generating any graphs. Any log-in attempt longer than five minutes was disregarded, since it may have been a mistake caused by the user during testing (pause/stop test midway). **

## Direction Design Rationale

The direction-based password scheme is essentially a subset of text-based password schemes. Its aim is to leverage a user's natural concept of direction in order to create usable and functional passwords.



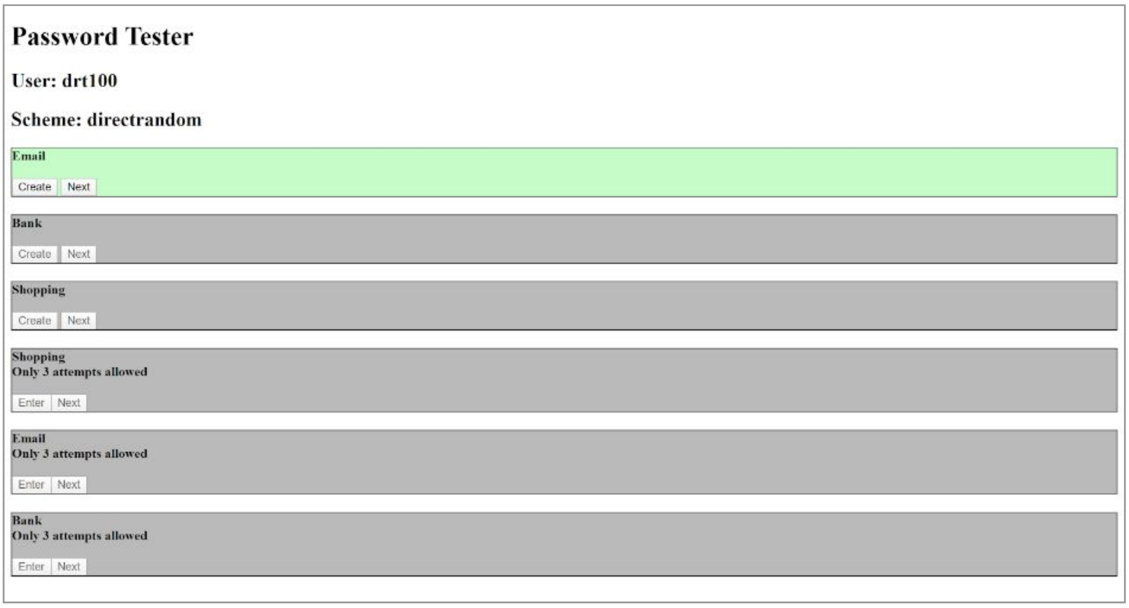
A compass showing eight distinct directions is used to help translate a sequence of arrows which represent a password, into the corresponding characters which are the actual password. These directions map to the letters [Q,W,E,A,D,Z,X,C], allowing users to enter passwords by typing on a keyboard. For instance, if the password scheme is asking for '↑' the user would input 'W', and so on. The letter "S" is not used but serves as the center of the compass.

An advantage of this scheme, is that the set of letters which make up all passwords are in very close proximity to each other on the keyboard. This encourages for faster attempt times as users don't have to move their hand at all while typing, only the fingers. All disadvantages of the text-based passwords scheme also apply to the direction-based scheme. This includes vulnerability to keylogger attacks and also revealing password length during creation/entry.

The size of the direction scheme is $8^n$, where *n* represents the length of the password. In our implementation, the maximum capacity of the scheme is $8^7 = (2^3)^7 = 2^{21}$. This means, that a total of 2,097,152 ($2^{21}$) distinct passwords can be generated for this particular scheme under the given constraints (length (n) is 7).

## Direction-based Password Implementation

The Direction-based password scheme works by using arrows to represent passwords and is implemented using Javascript and was hosted using Node.js. (Screenshot below)



### Password Tester

**User: drt100**

**Scheme: directrandom**

**Email**

**Bank**

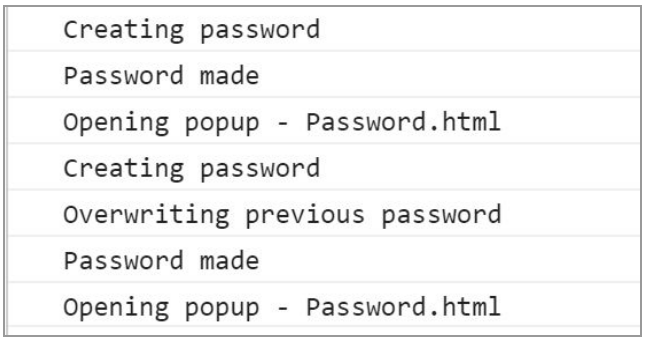
**Shopping**

**Shopping**
**Only 3 attempts allowed**

**Email**
**Only 3 attempts allowed**

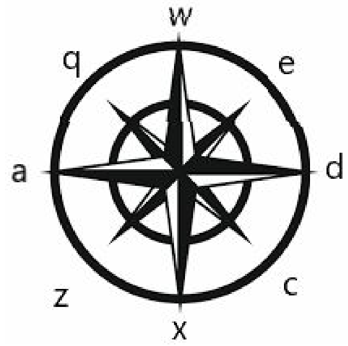
**Bank**
**Only 3 attempts allowed**

Passwords are created for users when the ‘Create’ button is clicked, triggering the randomization process responsible for generating passwords. After the process is complete, a testing window pops-up for users to practice and memorize their password. These actions/events generate log data that can be tracked in the Console/Terminal and stored in log files.

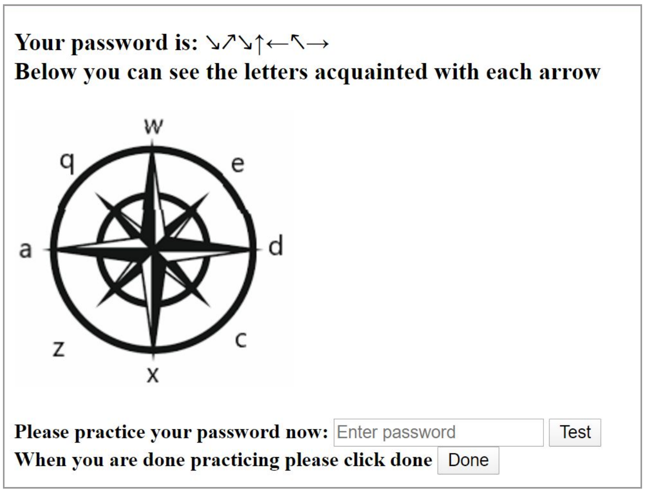


```
Creating password
Password made
Opening popup - Password.html
Creating password
Overwriting previous password
Password made
Opening popup - Password.html
```

Randomization works by choosing numbers from one to eight where every possible choice is a direction. A combination of seven directions makes up a single password and to represent these directions, the letters [q,w,e,a,d,z,x,c] are used to translate directional information into characters. A compass is used and serves as a visual aide for users during translation, either from directions to letters or vice versa.



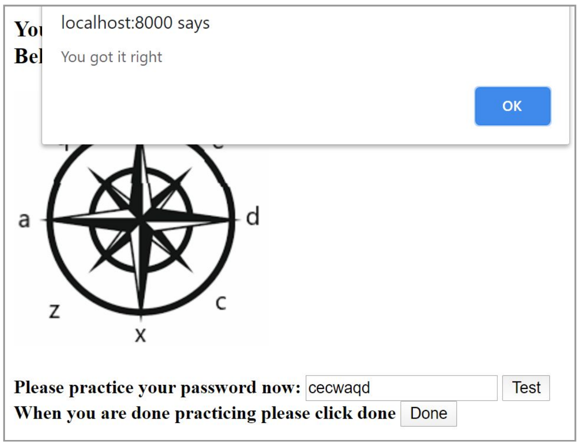
Passwords are requested from the user twice, once during creation and then at submission. Generated passwords appear as a sequence of arrows, the compass translates the arrows into letter representations that are then entered as the password. Practicing is meant to assist users in memorizing their newly created password, they also have the freedom to test their new password as many times as they would like.



**Your password is: ↘↗↘↑←↖→**
**Below you can see the letters acquainted with each arrow**

**Please practice your password now:** Enter password

**When you are done practicing please click done**



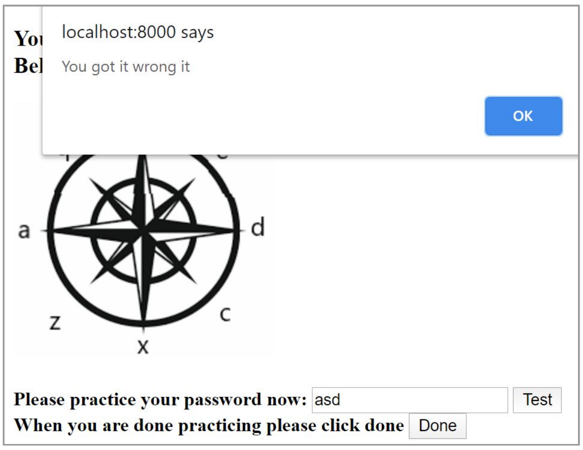
**You**
**Bel**

localhost:8000 says

You got it right

**Please practice your password now:** cecwaqd

**When you are done practicing please click done**



**You**
**Bel**

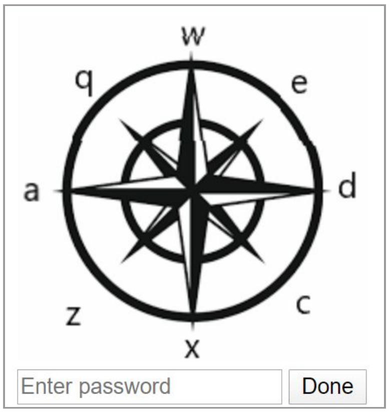
localhost:8000 says

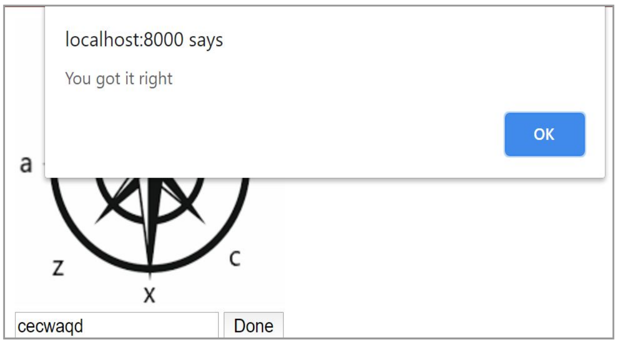
You got it wrong it

**Please practice your password now:** asd

**When you are done practicing please click done**

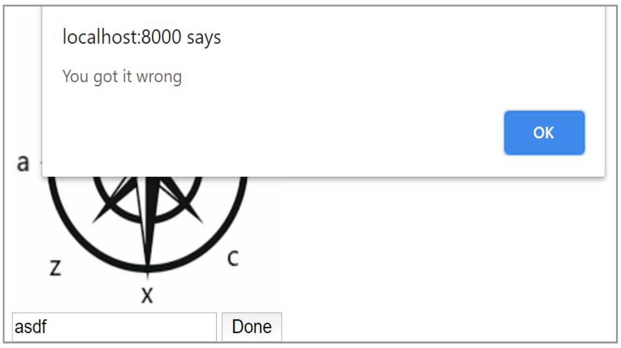
The submission pop-up works similarly, a compass is again provided to assist during the process. Users are now required to enter their random passwords created earlier. This time they only get 3 attempts for each password.




localhost:8000 says

You got it right

cecwaqd


localhost:8000 says

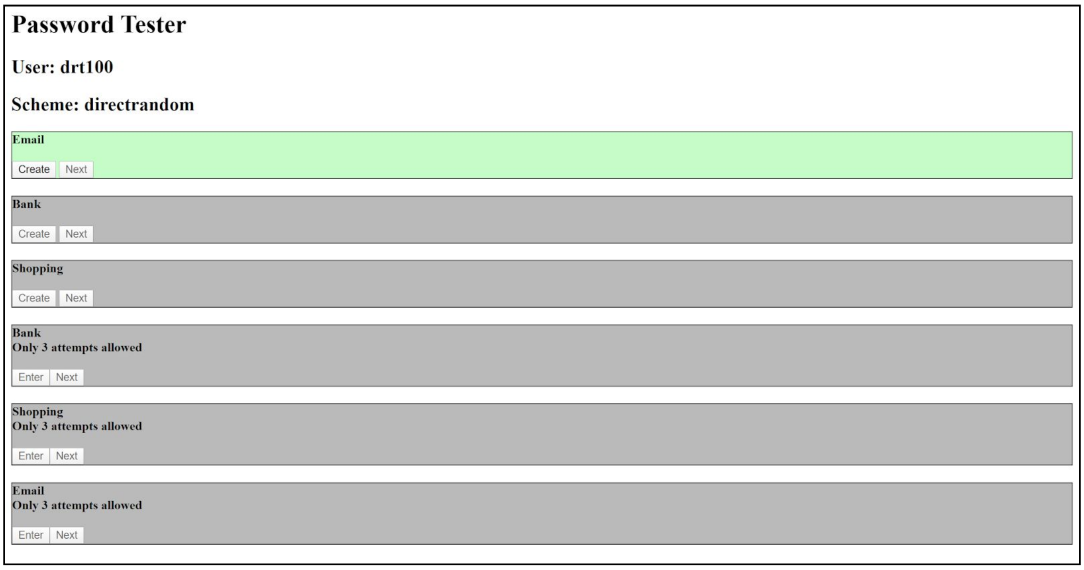
You got it wrong

asdf

After clicking ‘Done’ a notification informing users of the log-in  result is displayed.

## Direction-based Framework

Users are directed to the screen below when testing the password scheme. They start off by creating 3 different passwords for email, bank and shopping accounts. The passwords are randomly generated directions users must remember during the testing period. As testing takes place, all interactional data is logged and stored by the framework into CSV files for analysis later. Password submission occurs after the creation process, this is where a scheme's usability is truly tested. Timestamps included in the logged data, allow for determining the time it takes for users to enter a password. Information such as the results of a submission either success or failure is also logged. These time intervals provide details into how long users take when signing into an account using the direction-based scheme.



Password Tester

User: drt100

Scheme: directrandom

Email

Bank

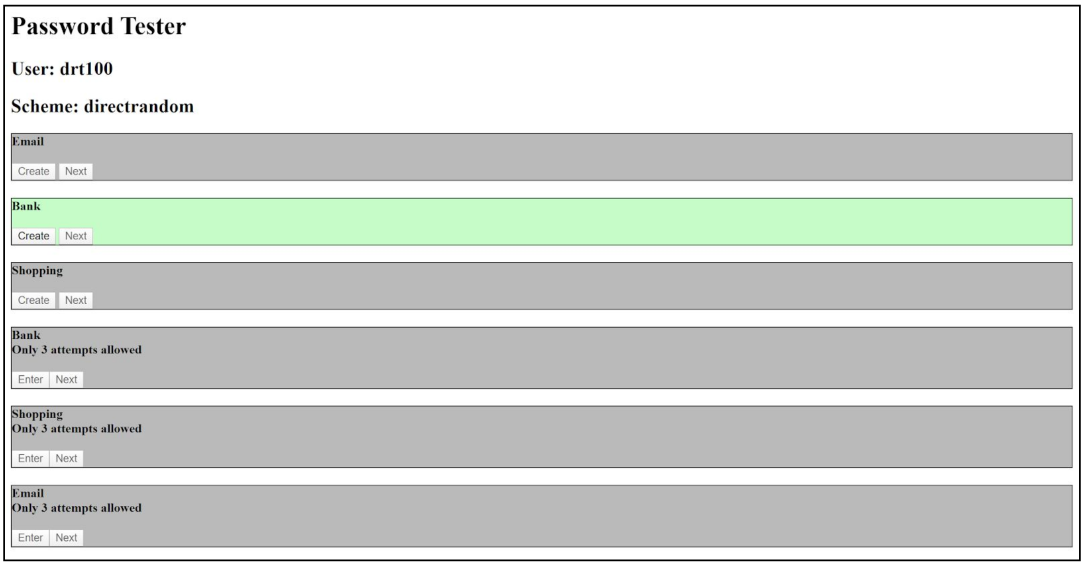
Shopping

Bank
Only 3 attempts allowed

Shopping
Only 3 attempts allowed

Email
Only 3 attempts allowed

Selecting 'Create' triggers the practice pop-up to launch. 'Create' can be clicked multiple times, and for each click, a new randomized password is created and overwritten to replace the previous.



Password Tester

User: drt100

Scheme: directrandom

Email

Bank

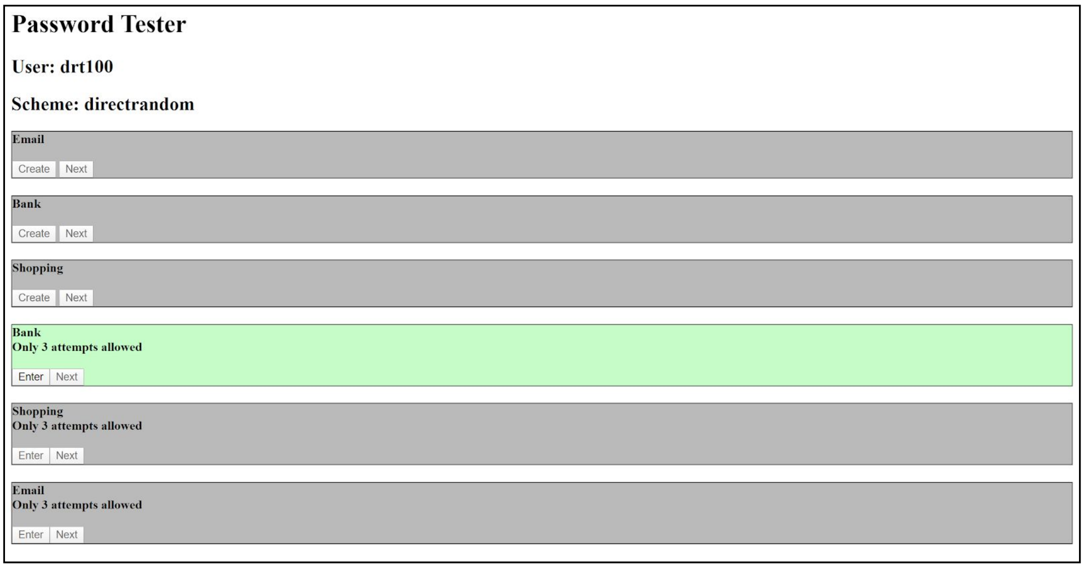
Shopping

Bank
Only 3 attempts allowed

Shopping
Only 3 attempts allowed

Email
Only 3 attempts allowed

Selecting ‘Enter’ triggers the submission pop-up to launch. This is where users get to enter their generated passwords one by one. Each section allows for a maximum of 3 attempts regardless of success or failure.


Password Tester

User: drt100

Scheme: directrandom

Email

Bank

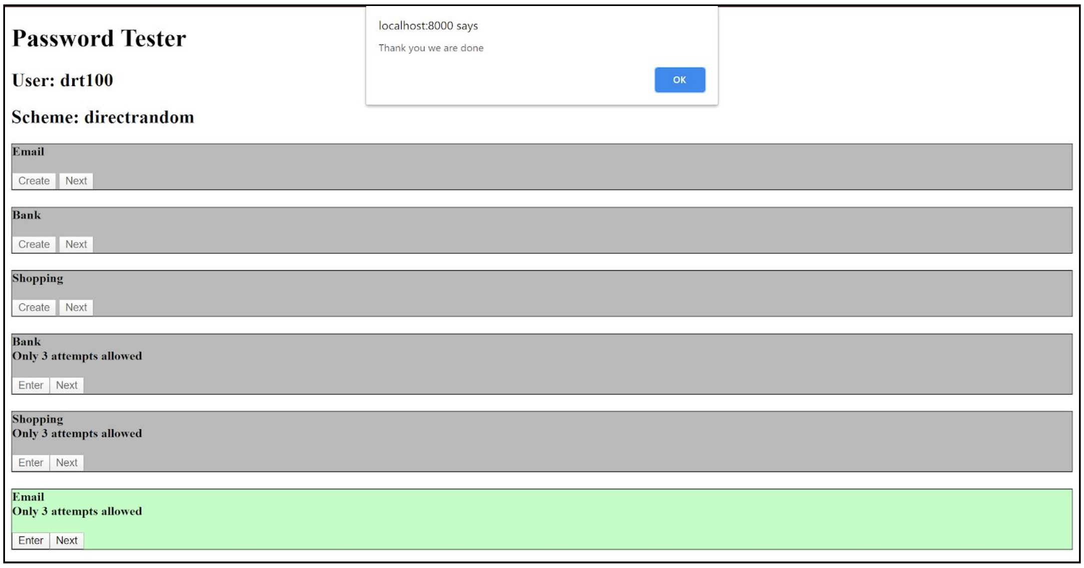
Shopping

Bank
Only 3 attempts allowed

Shopping
Only 3 attempts allowed

Email
Only 3 attempts allowed

Clicking ‘Next’  informs the program that the user is finished with the current section. As a result, the next section is enabled and at the end,  a thank you message is displayed.


localhost:8000 says

Thank you we are done

Password Tester

User: drt100

Scheme: directrandom

Email

Bank

Shopping

Bank
Only 3 attempts allowed

Shopping
Only 3 attempts allowed

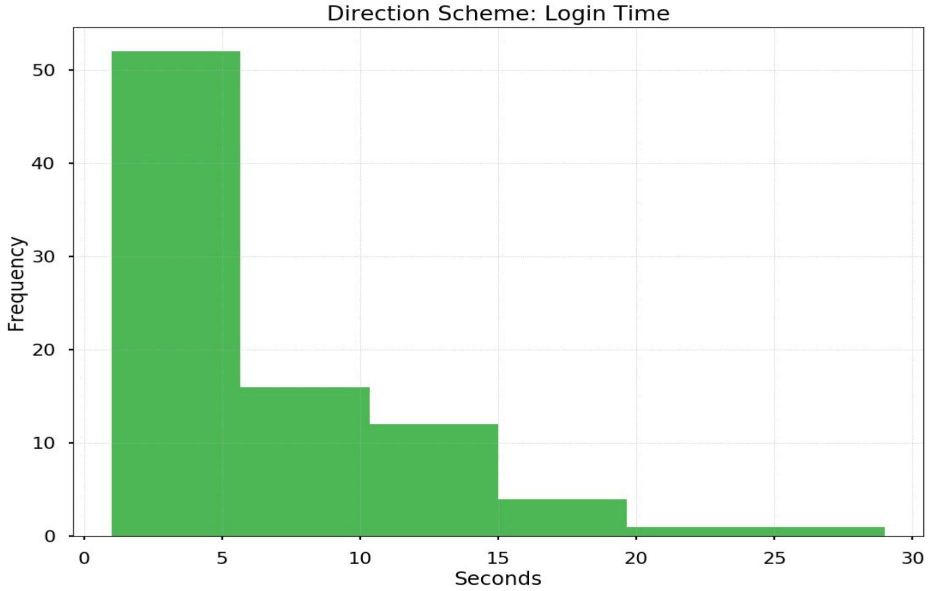
Email
Only 3 attempts allowed

## Direction Scheme Test Results

. Log data generated from the testing framework was used with the datalog software implemented in part A to compute and illustrate these statistics.

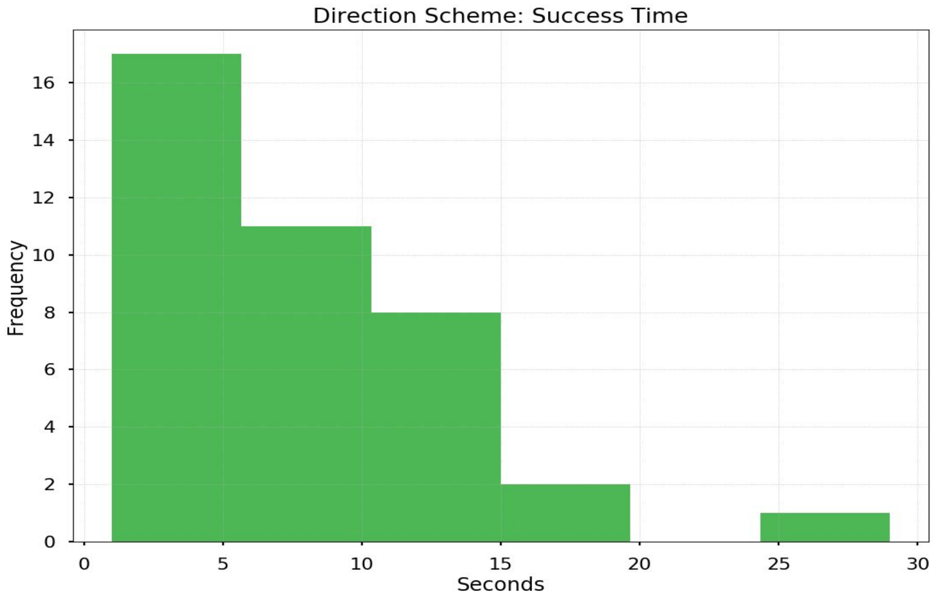
| | Direction-Based |
|---|---|
| Mean # of Attempts: | **5** |
| Mean # of Successes: | **2** |
| Mean # of Failures: | **3** |
| Mean Login Time: | **9s** |
| Mean Successes Time: | **12s** |
| Mean Failures Time: | **7s** |

The averages computed above show that users overall were not accurate when using directional passwords. Yet, still managed to enter passwords close to the same speed as they would for text passwords. This comes at no surprise, since direction-based passwords are a subset of text-based passwords, both schemes require keyboards, and naturally produce similar log-in times.

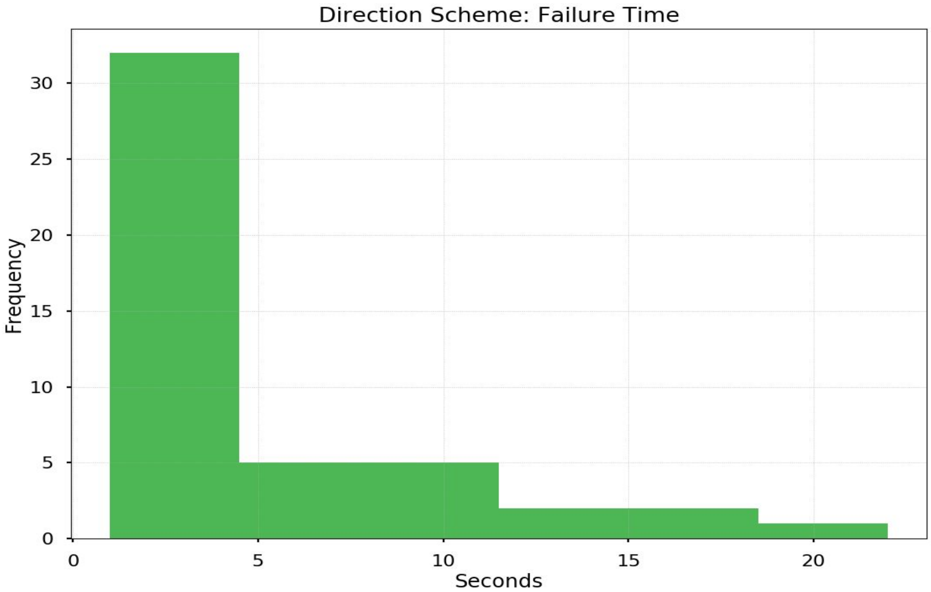


The majority of users were able to enter their passwords in under 5 seconds, a bit faster than the text-based scheme. Reaffirming, that the use of directions was received well by test participants.

The 'Mean Login Time' of directional and text passwords were also close, at 9 seconds (direction) and 10 seconds (text).



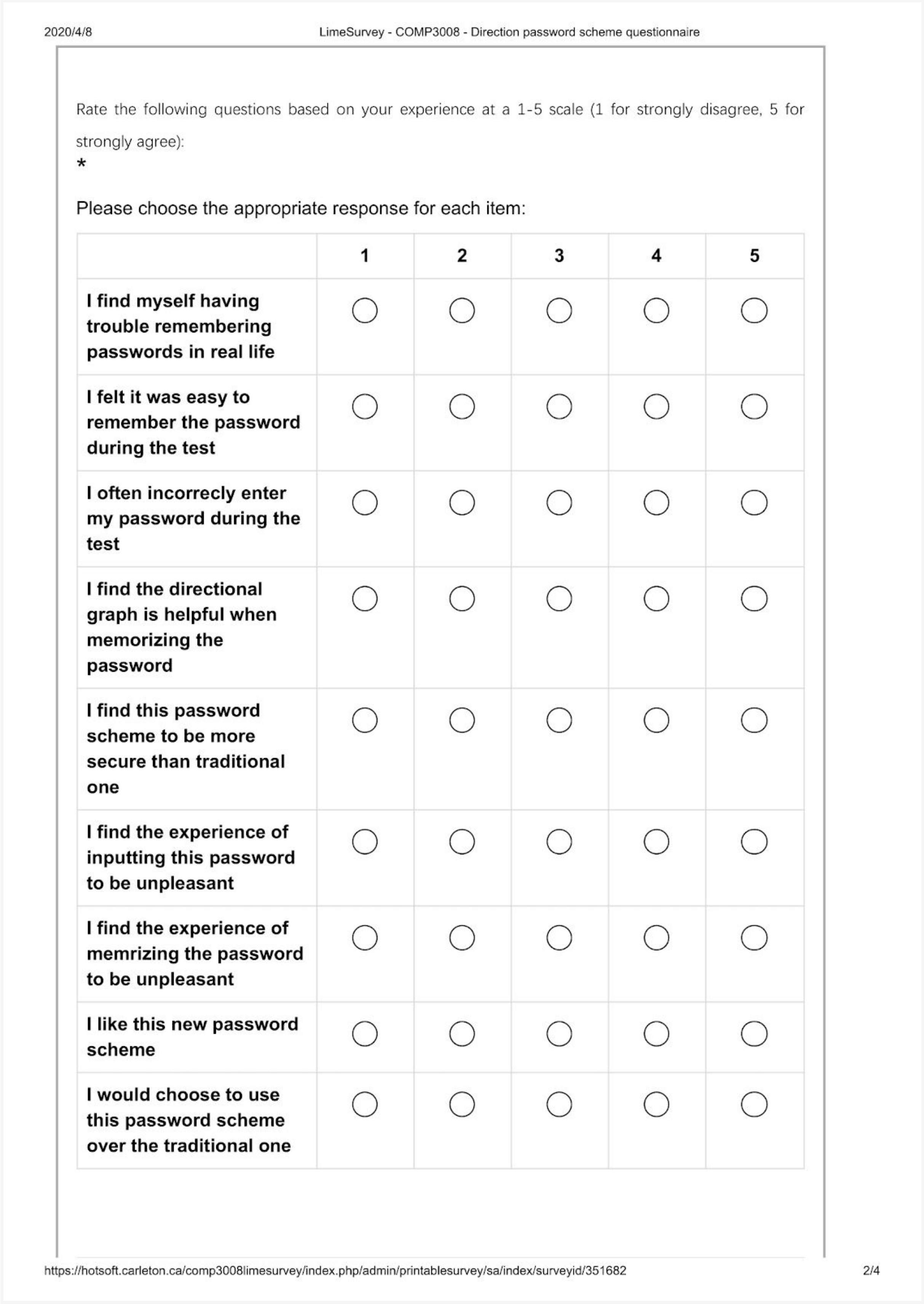
Successful log-ins mostly occurred at the 5 seconds mark, again slightly faster than the text scheme. The 'Mean Successes Time' of both were 12 seconds (direction) and 10 seconds (text).



Failure times of the direction-based password again occurred much faster than that of text-based passwords. The majority of failures were under 5 seconds for directional and just over 5 seconds for text. The 'Mean Failure Time' equalled 7 seconds (directional) and 12 seconds (text).

In conclusion, direction-based passwords were just as fast as text-based passwords but, a lot less accurate.

# Questionnaire



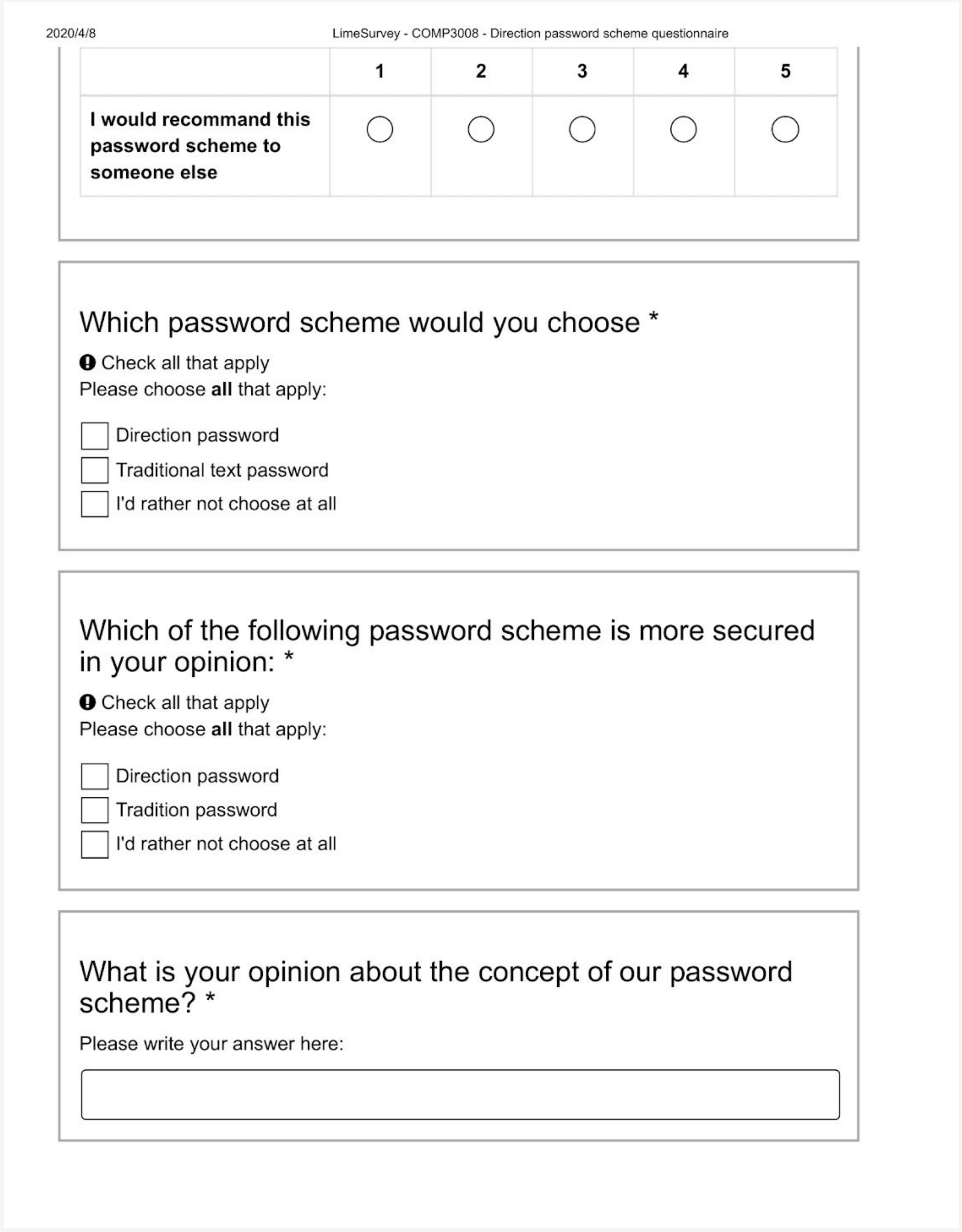
2020/4/8 LimeSurvey - COMP3008 - Direction password scheme questionnaire

Rate the following questions based on your experience at a 1-5 scale (1 for strongly disagree, 5 for strongly agree):
*

Please choose the appropriate response for each item:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **I find myself having trouble remembering passwords in real life** | ○ | ○ | ○ | ○ | ○ |
| **I felt it was easy to remember the password during the test** | ○ | ○ | ○ | ○ | ○ |
| **I often incorrecly enter my password during the test** | ○ | ○ | ○ | ○ | ○ |
| **I find the directional graph is helpful when memorizing the password** | ○ | ○ | ○ | ○ | ○ |
| **I find this password scheme to be more secure than traditional one** | ○ | ○ | ○ | ○ | ○ |
| **I find the experience of inputting this password to be unpleasant** | ○ | ○ | ○ | ○ | ○ |
| **I find the experience of memrizing the password to be unpleasant** | ○ | ○ | ○ | ○ | ○ |
| **I like this new password scheme** | ○ | ○ | ○ | ○ | ○ |
| **I would choose to use this password scheme over the traditional one** | ○ | ○ | ○ | ○ | ○ |

https://hotsoft.carleton.ca/comp3008limesurvey/index.php/admin/printablesurvey/sa/index/surveyid/351682 2/4



2020/4/8 LimeSurvey - COMP3008 - Direction password scheme questionnaire

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **I would recommand this password scheme to someone else** | ○ | ○ | ○ | ○ | ○ |

Which password scheme would you choose *

❗ Check all that apply

Please choose **all** that apply:

□ Direction password

□ Traditional text password

□ I'd rather not choose at all

Which of the following password scheme is more secured in your opinion: *

❗ Check all that apply

Please choose **all** that apply:

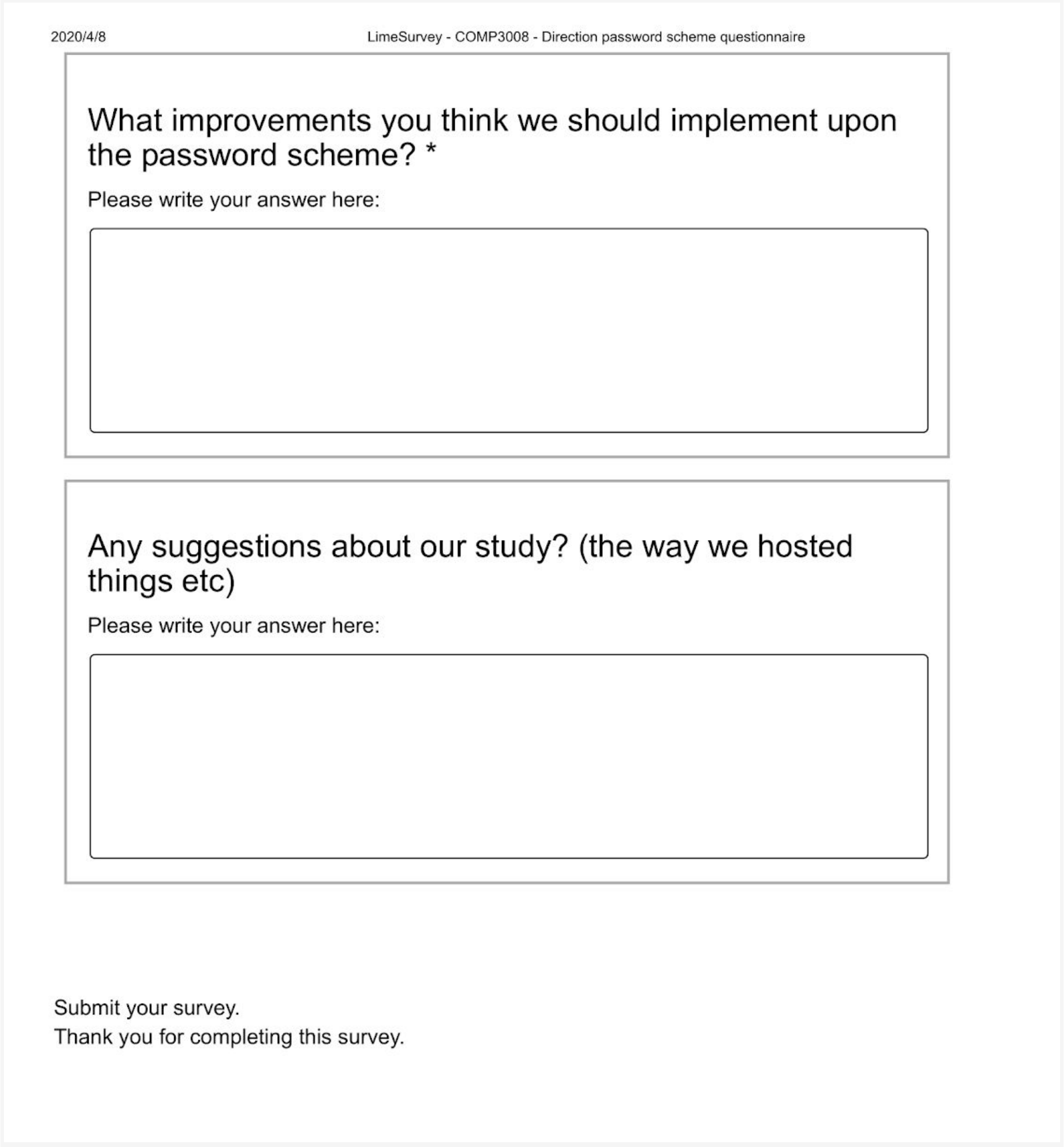
□ Direction password

□ Tradition password

□ I'd rather not choose at all

What is your opinion about the concept of our password scheme? *

Please write your answer here:



2020/4/8 LimeSurvey - COMP3008 - Direction password scheme questionnaire

What improvements you think we should implement upon the password scheme? *

Please write your answer here:

Any suggestions about our study? (the way we hosted things etc)

Please write your answer here:

Submit your survey.
Thank you for completing this survey.

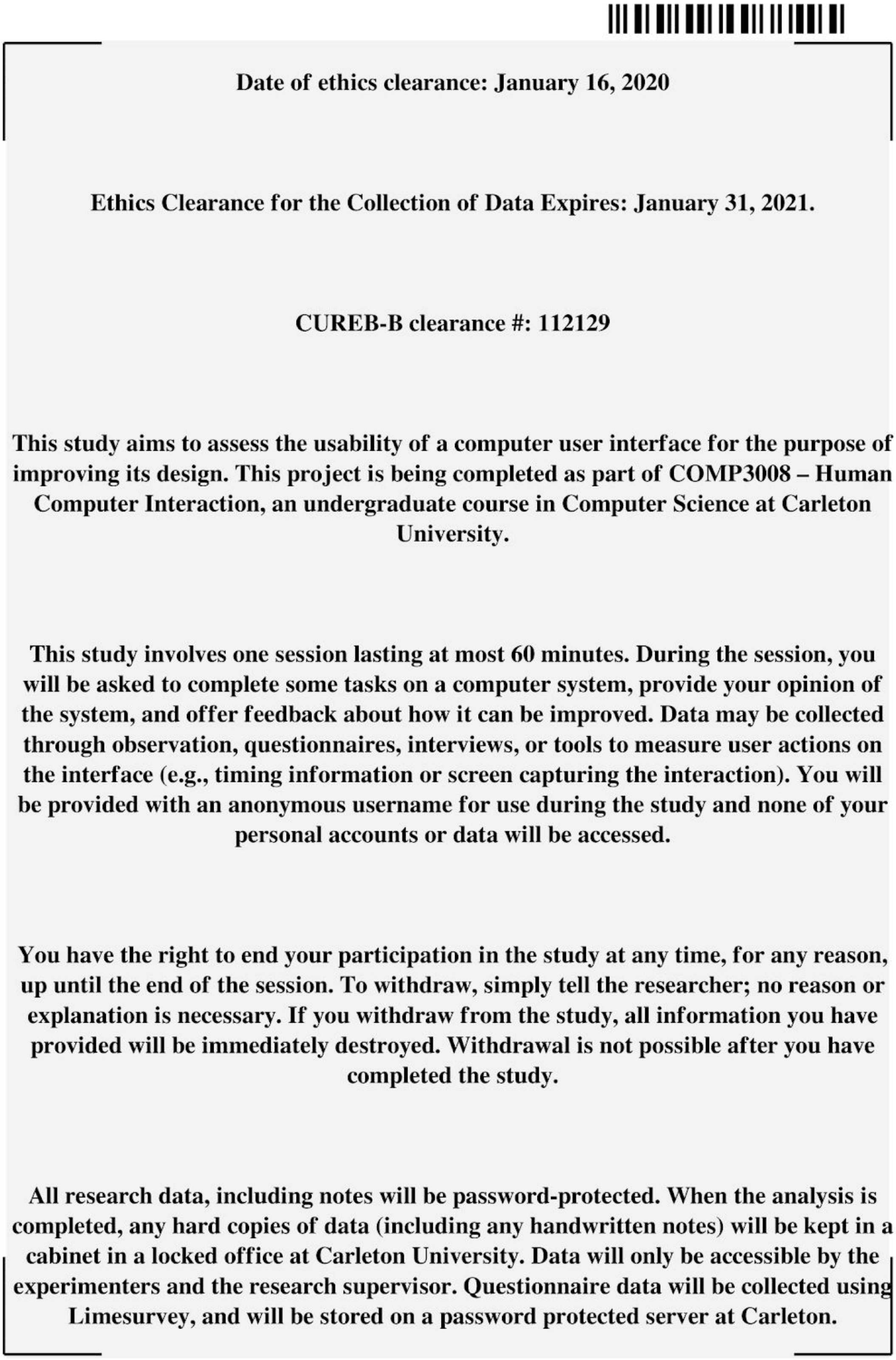
**URL:**

https://hotsoft.carleton.ca/comp3008limesurvey/index.php/351682?token=XENaPcKbkz5ZvAb&newtest=Y

# Appendix

Consent forms

URL: https://hotsoft.carleton.ca/comp3008limesurvey/index.php/956838?lang=en



Date of ethics clearance: January 16, 2020

Ethics Clearance for the Collection of Data Expires: January 31, 2021.

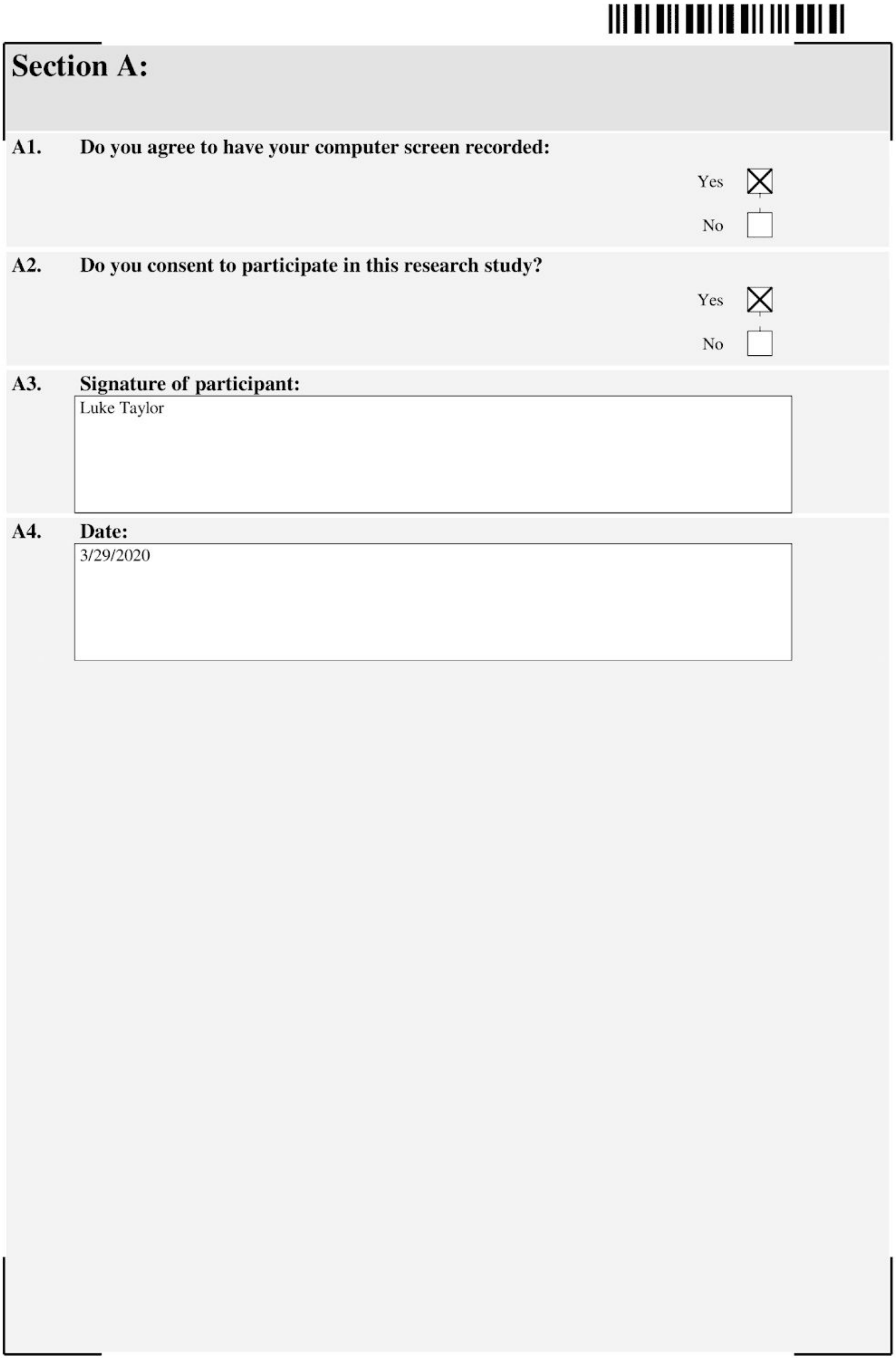
CUREB-B clearance #: 112129

This study aims to assess the usability of a computer user interface for the purpose of improving its design. This project is being completed as part of COMP3008 – Human Computer Interaction, an undergraduate course in Computer Science at Carleton University.

This study involves one session lasting at most 60 minutes. During the session, you will be asked to complete some tasks on a computer system, provide your opinion of the system, and offer feedback about how it can be improved. Data may be collected through observation, questionnaires, interviews, or tools to measure user actions on the interface (e.g., timing information or screen capturing the interaction). You will be provided with an anonymous username for use during the study and none of your personal accounts or data will be accessed.

You have the right to end your participation in the study at any time, for any reason, up until the end of the session. To withdraw, simply tell the researcher; no reason or explanation is necessary. If you withdraw from the study, all information you have provided will be immediately destroyed. Withdrawal is not possible after you have completed the study.

All research data, including notes will be password-protected. When the analysis is completed, any hard copies of data (including any handwritten notes) will be kept in a cabinet in a locked office at Carleton University. Data will only be accessible by the experimenters and the research supervisor. Questionnaire data will be collected using Limesurvey, and will be stored on a password protected server at Carleton.



## Section A:

**A1.** **Do you agree to have your computer screen recorded:**

Yes ☒

No □

**A2.** **Do you consent to participate in this research study?**

Yes ☒

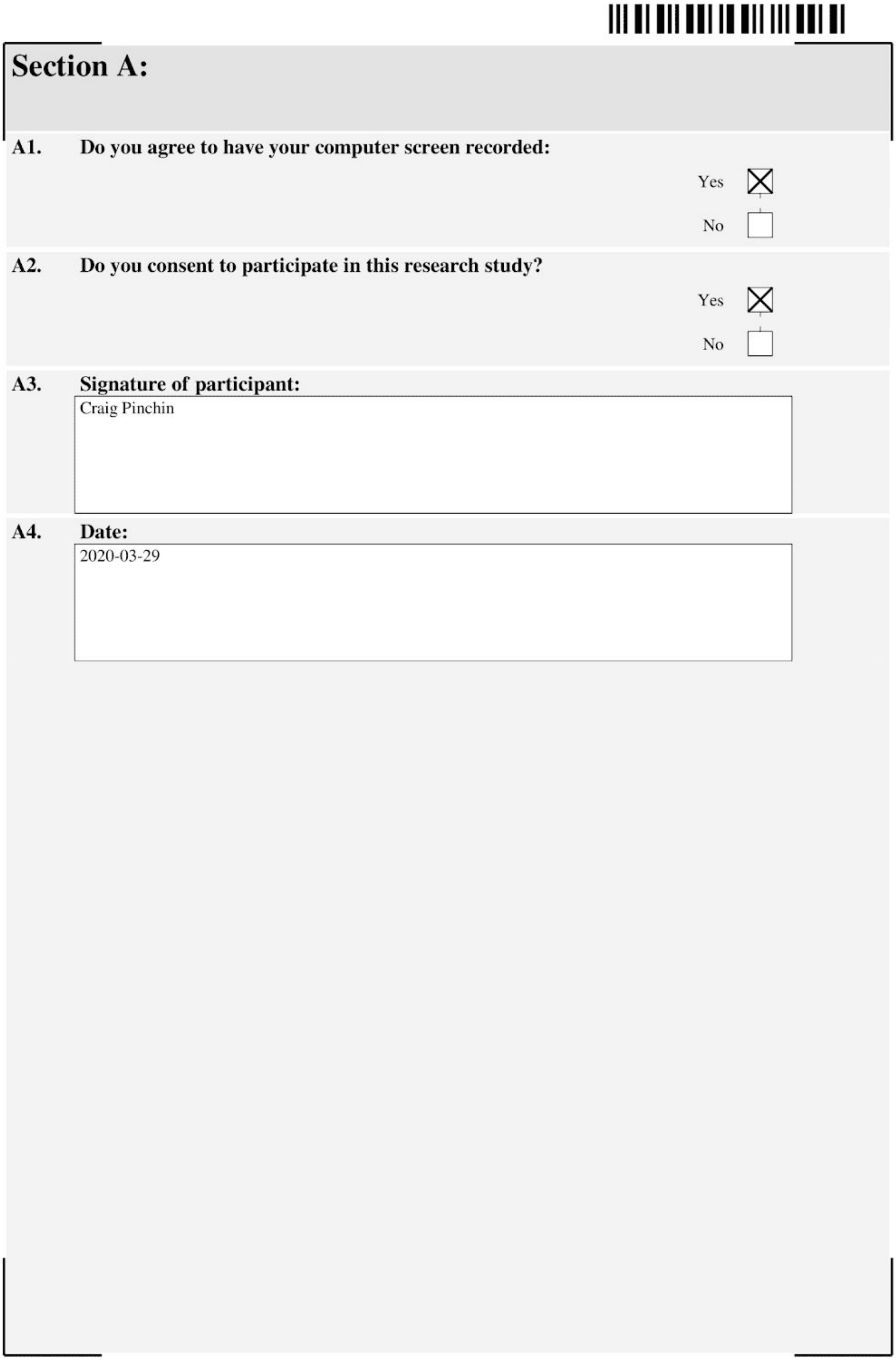
No □

**A3.** **Signature of participant:**

Luke Taylor

**A4.** **Date:**

3/29/2020



## Section A:

**A1.** **Do you agree to have your computer screen recorded:**

Yes ☒

No □

**A2.** **Do you consent to participate in this research study?**

Yes ☒

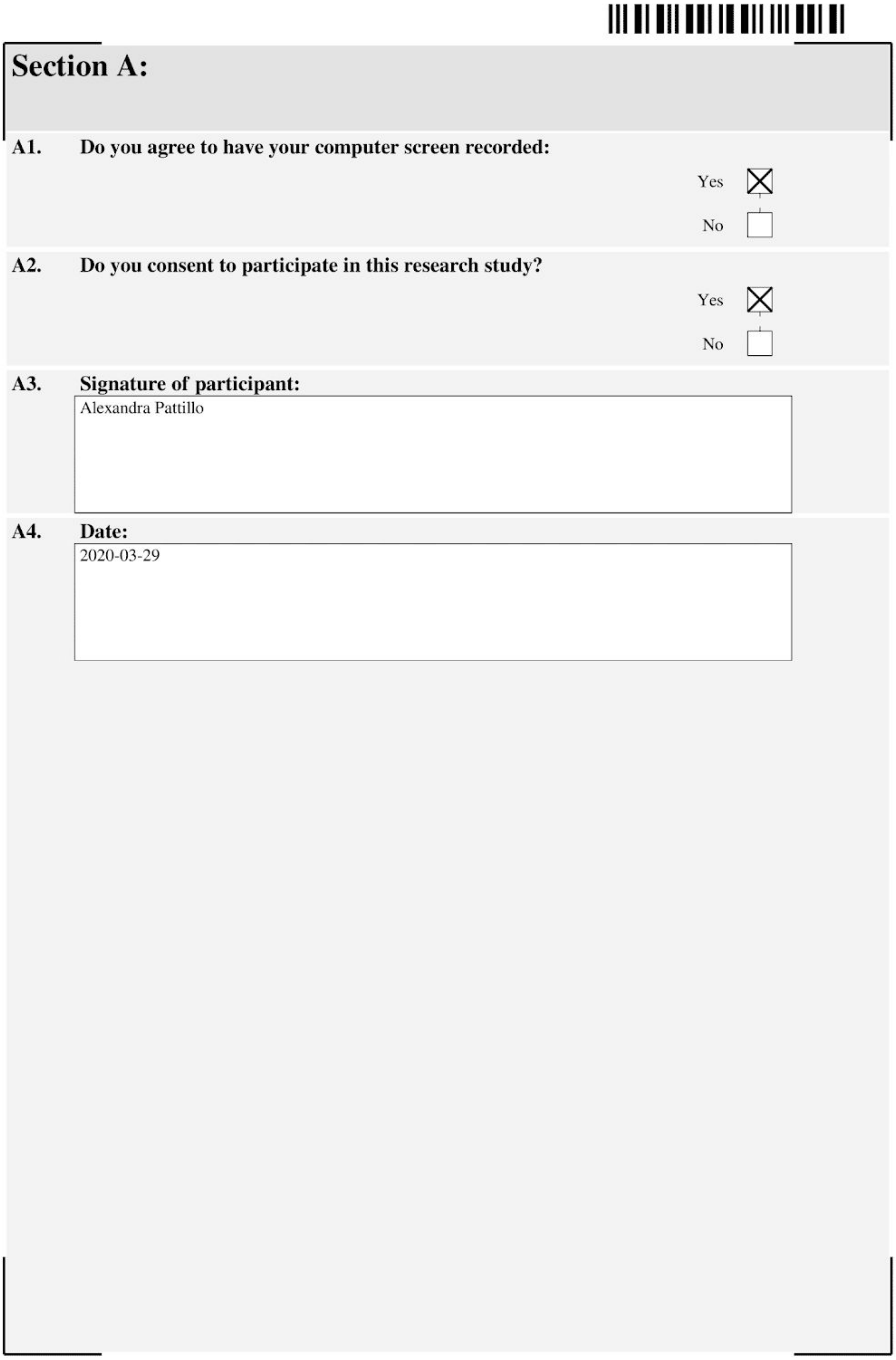
No □

**A3.** **Signature of participant:**

Craig Pinchin

**A4.** **Date:**

2020-03-29



## Section A:

A1. **Do you agree to have your computer screen recorded:**

Yes ☒

No □

A2. **Do you consent to participate in this research study?**

Yes ☒

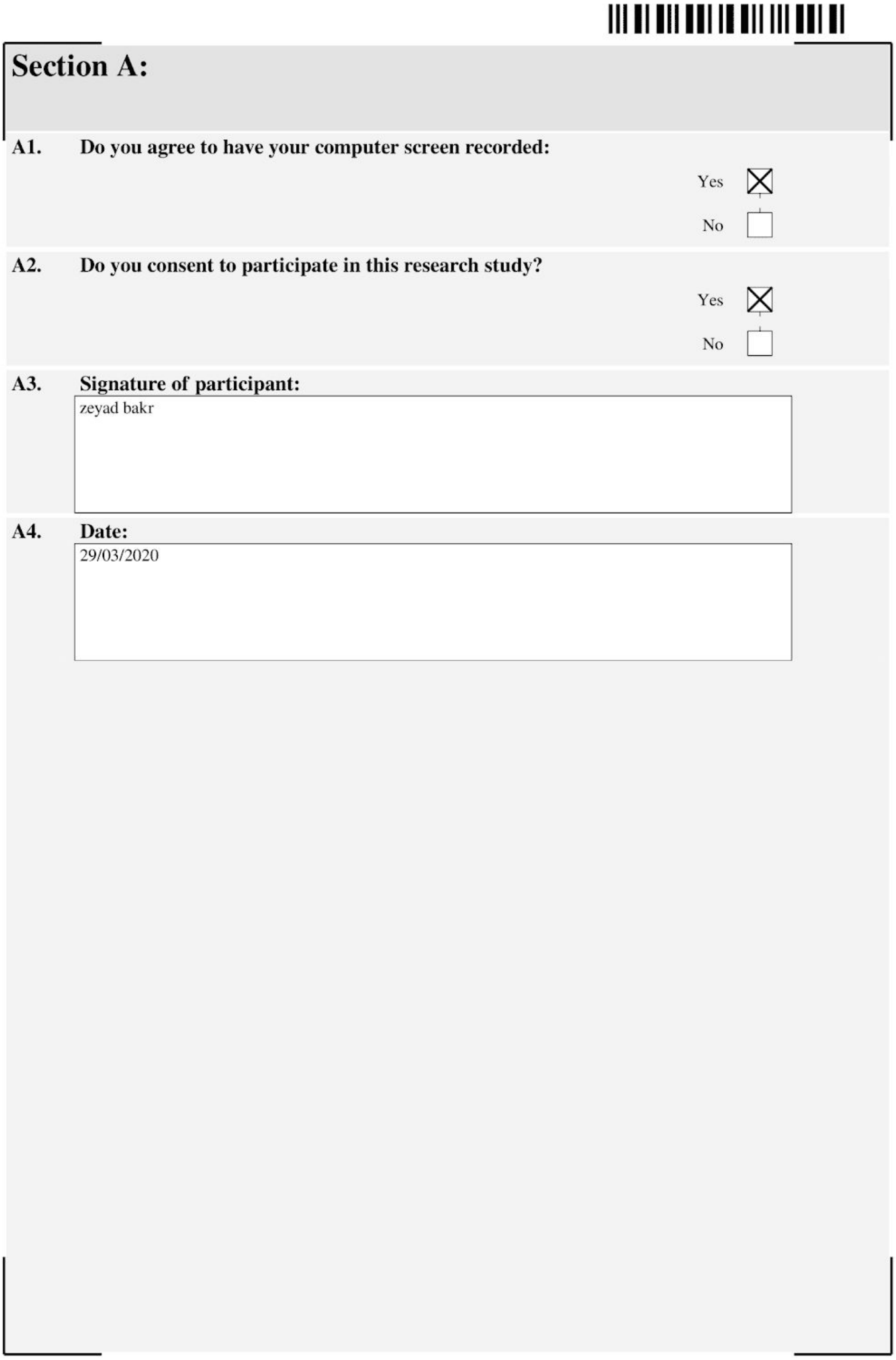
No □

A3. **Signature of participant:**

Alexandra Pattillo

A4. **Date:**

2020-03-29



## Section A:

A1. **Do you agree to have your computer screen recorded:**

Yes ☒

No □

A2. **Do you consent to participate in this research study?**

Yes ☒

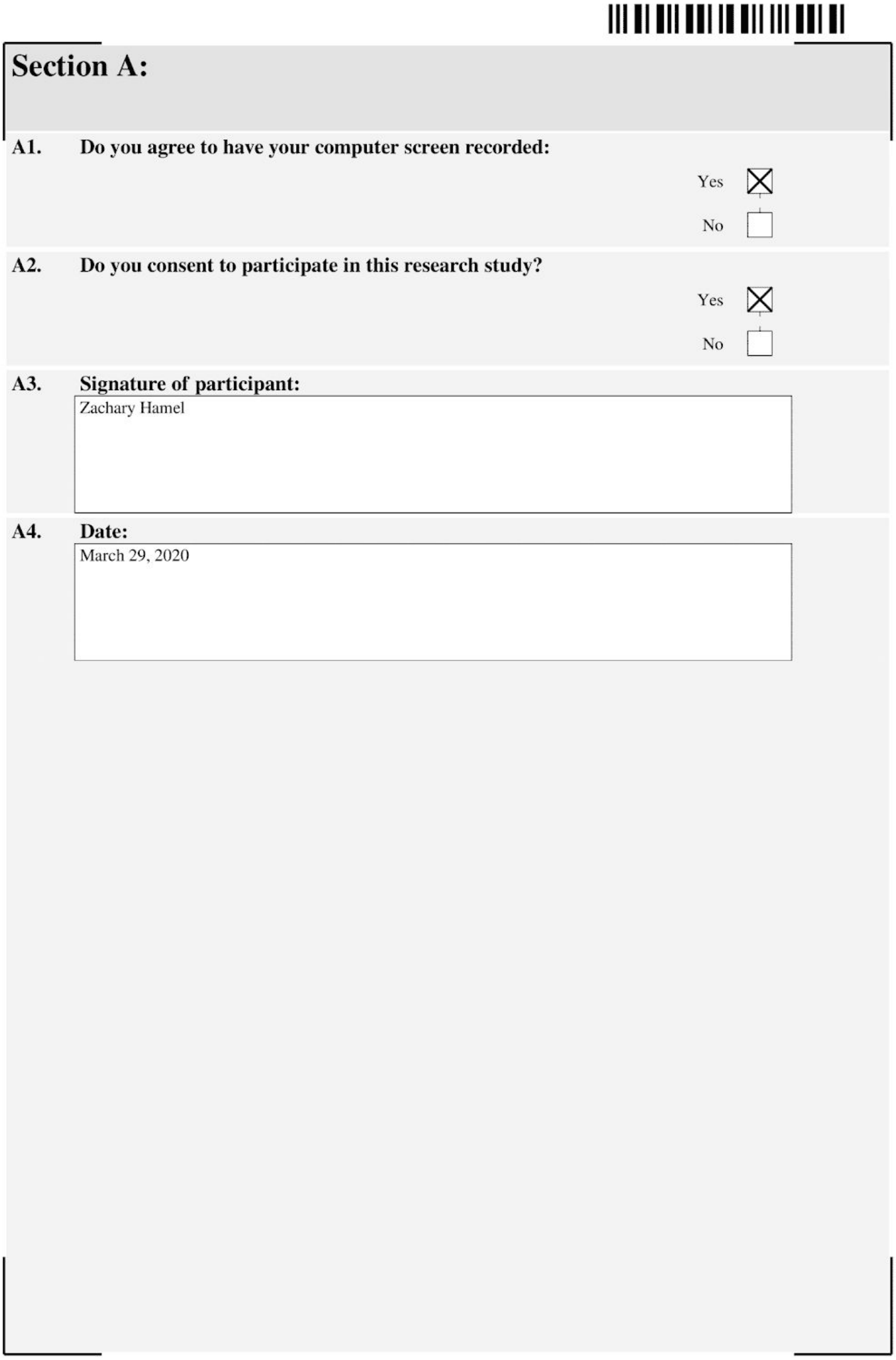
No □

A3. **Signature of participant:**

zeyad bakr

A4. **Date:**

29/03/2020



## Section A:

A1. **Do you agree to have your computer screen recorded:**

Yes ☒

No □

A2. **Do you consent to participate in this research study?**

Yes ☒

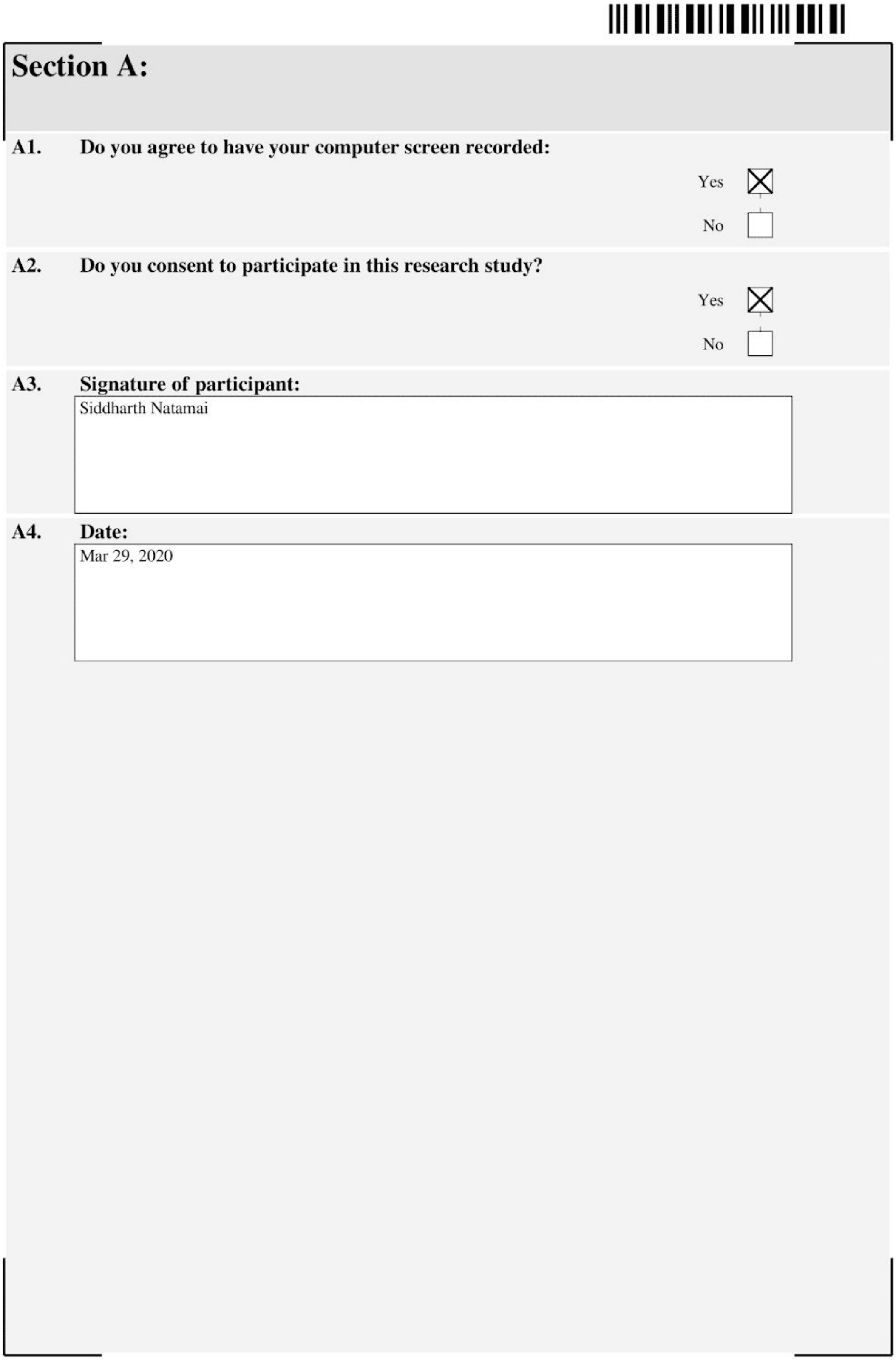
No □

A3. **Signature of participant:**

Zachary Hamel

A4. **Date:**

March 29, 2020



## Section A:

A1. **Do you agree to have your computer screen recorded:**

Yes ☒

No □

A2. **Do you consent to participate in this research study?**

Yes ☒

No □

A3. **Signature of participant:**

Siddharth Natamai

A4. **Date:**

Mar 29, 2020

## Section A:

**A1. Do you agree to have your computer screen recorded:**

Yes ☒

No □

**A2. Do you consent to participate in this research study?**

Yes □

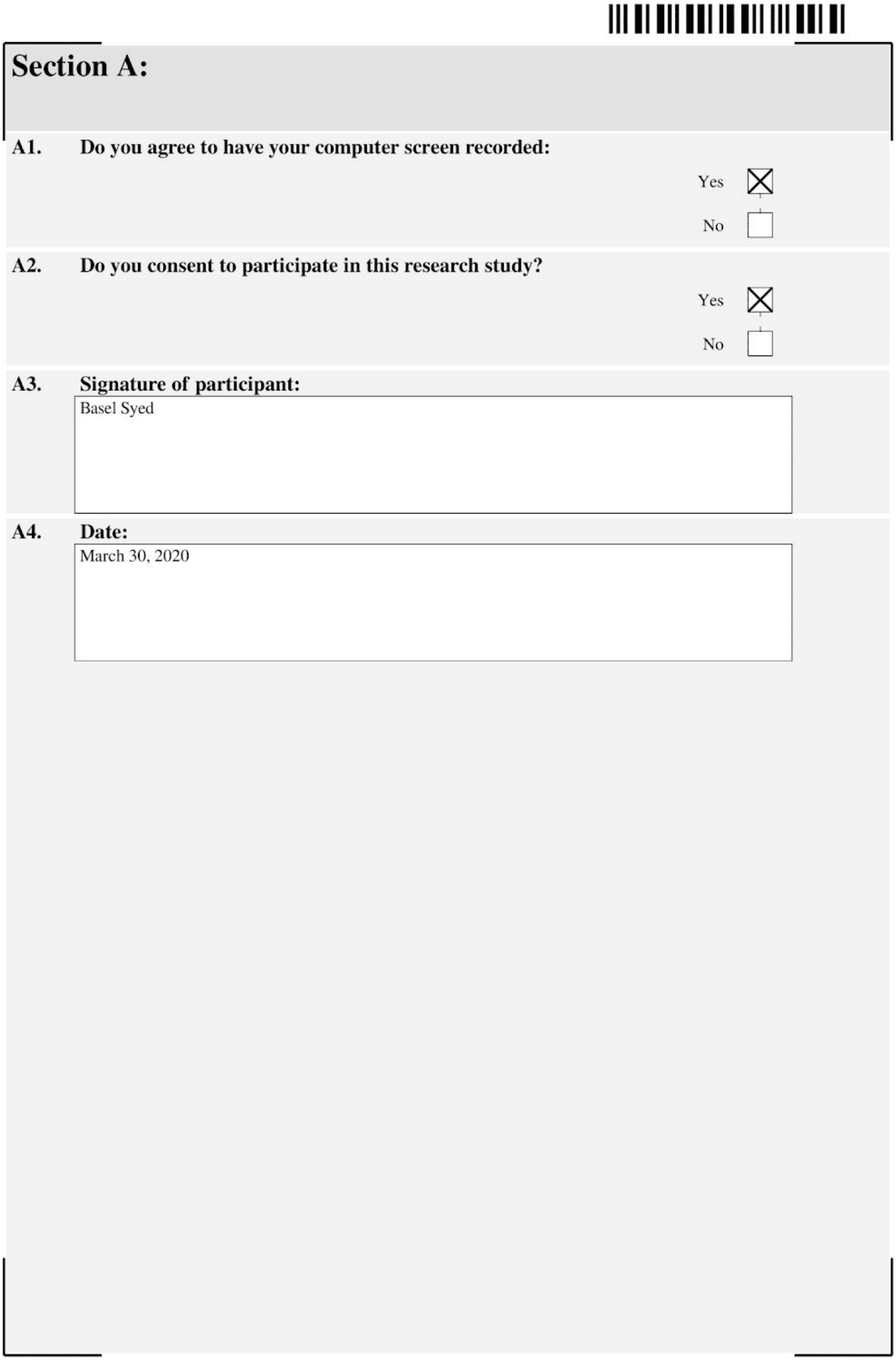
No ☒

**A3. Signature of participant:**

Elijah Mendez

**A4. Date:**

March 29th 2020



## Section A:

A1. **Do you agree to have your computer screen recorded:**

Yes ☒

No □

A2. **Do you consent to participate in this research study?**

Yes ☒

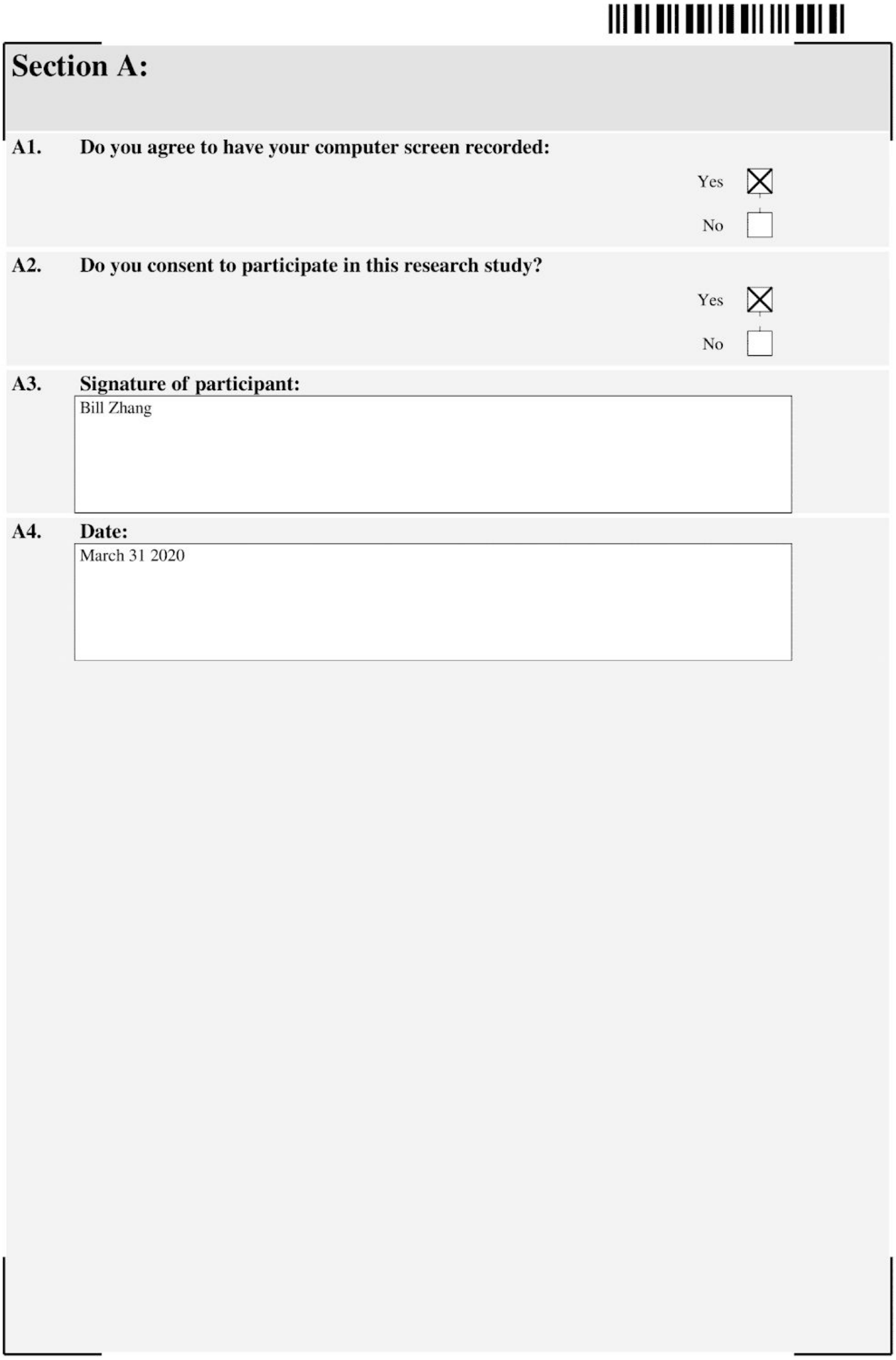
No □

A3. **Signature of participant:**

Basel Syed

A4. **Date:**

March 30, 2020



## Section A:

A1. **Do you agree to have your computer screen recorded:**

Yes ☒

No □

A2. **Do you consent to participate in this research study?**

Yes ☒

No □

A3. **Signature of participant:**

Bill Zhang

A4. **Date:**

March 31 2020

## Section A:

**A1.** **Do you agree to have your computer screen recorded:**

Yes ☒

No □

**A2.** **Do you consent to participate in this research study?**

Yes ☒

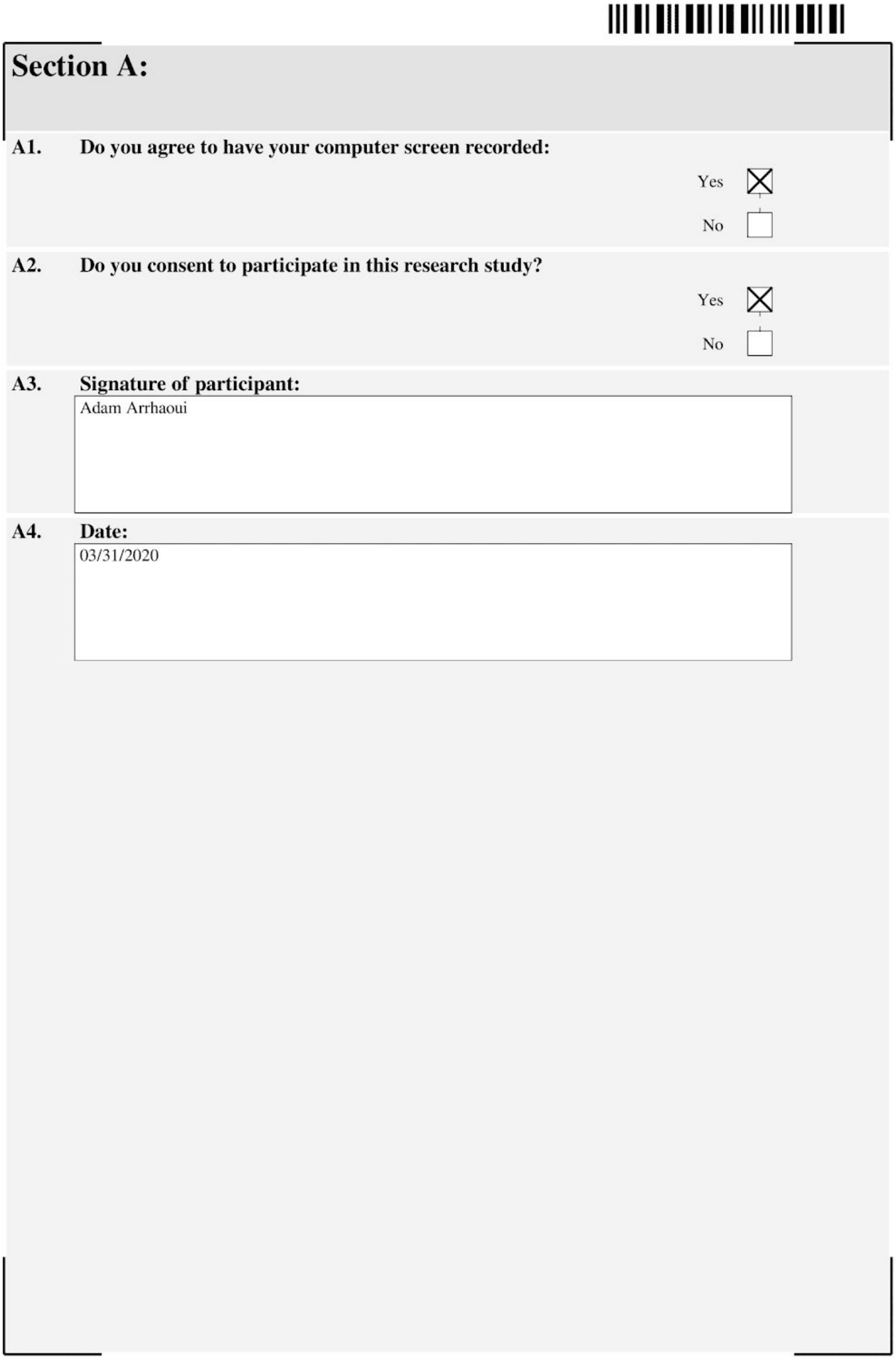
No □

**A3.** **Signature of participant:**

C Stolwyk

**A4.** **Date:**

March 31 2020



## Section A:

**A1. Do you agree to have your computer screen recorded:**

Yes ☒

No □

**A2. Do you consent to participate in this research study?**

Yes ☒

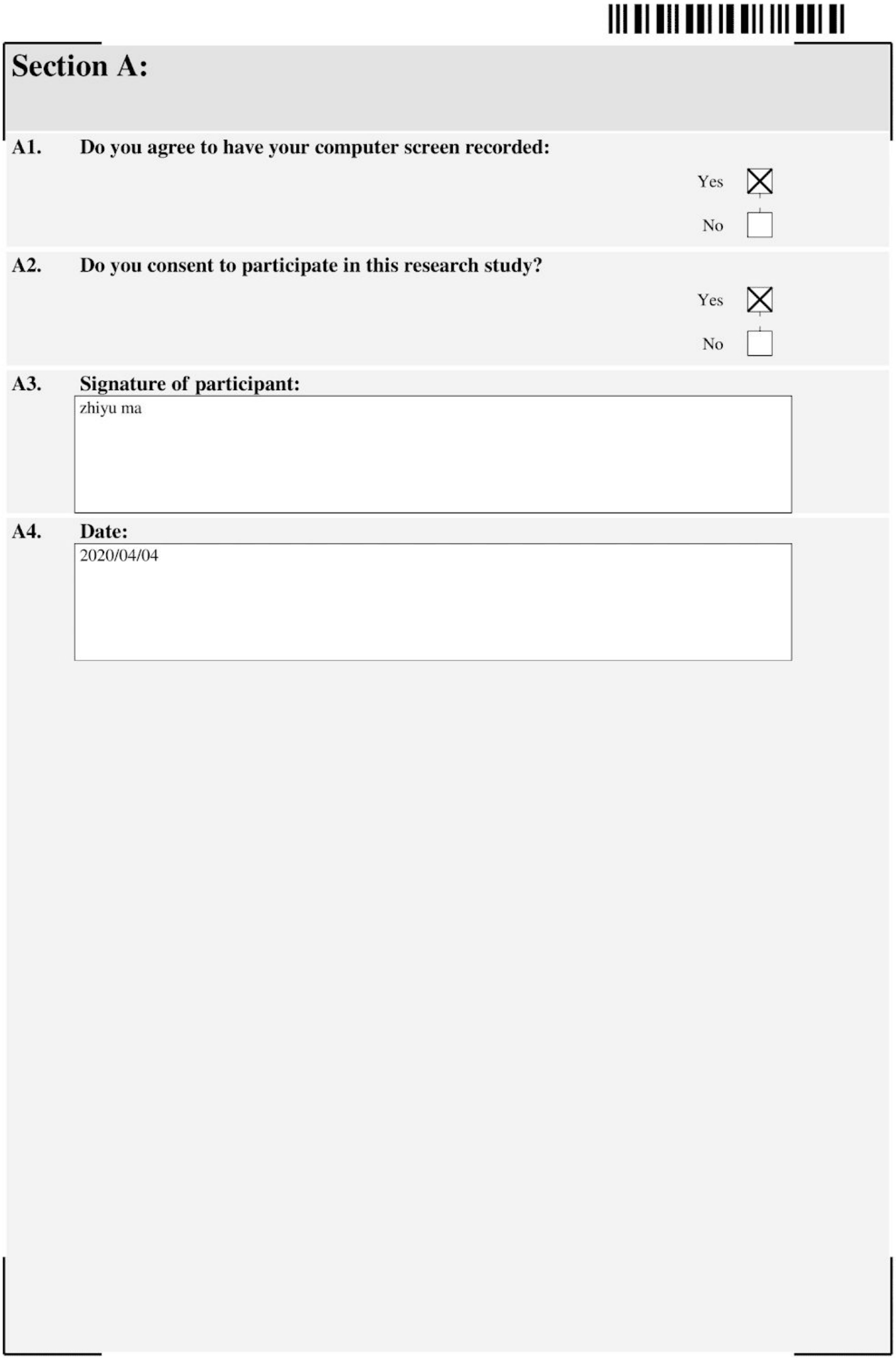
No □

**A3. Signature of participant:**

Adam Arrhaoui

**A4. Date:**

03/31/2020



## Section A:

A1. **Do you agree to have your computer screen recorded:**

Yes ☒

No □

A2. **Do you consent to participate in this research study?**

Yes ☒

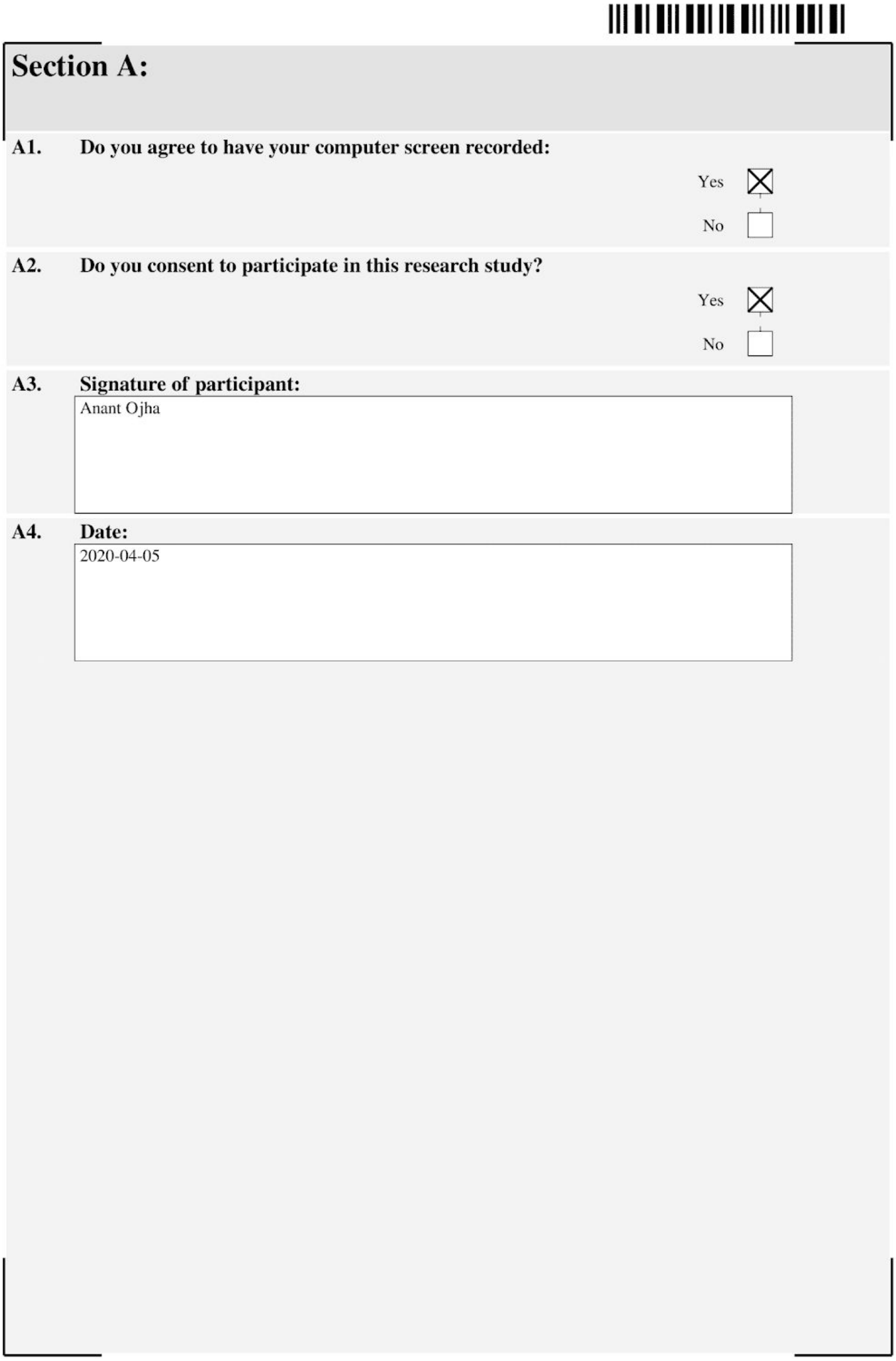
No □

A3. **Signature of participant:**

zhiyu ma

A4. **Date:**

2020/04/04



## Section A:

A1. **Do you agree to have your computer screen recorded:**

Yes ☒

No □

A2. **Do you consent to participate in this research study?**

Yes ☒

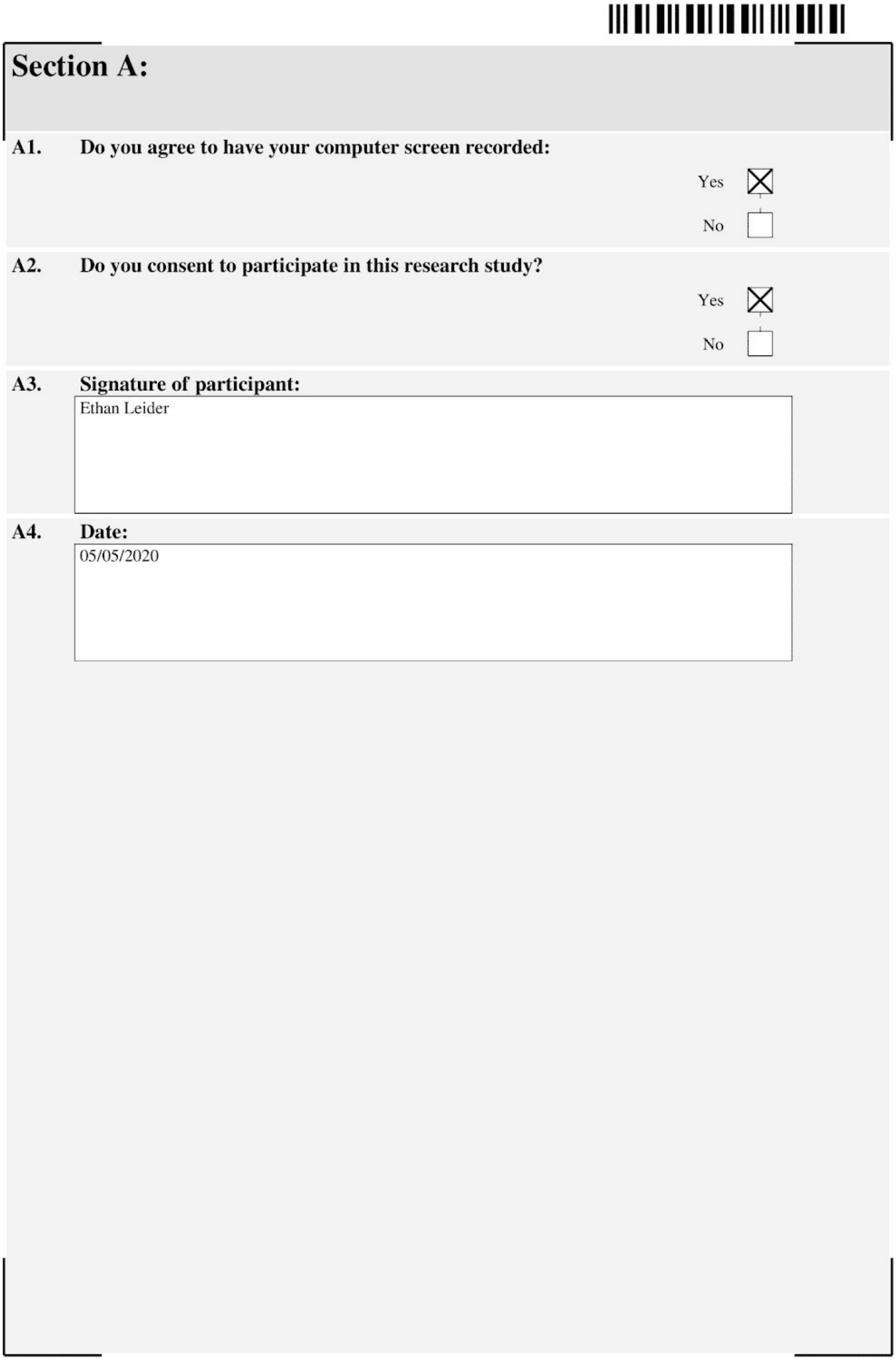
No □

A3. **Signature of participant:**

Anant Ojha

A4. **Date:**

2020-04-05



## Section A:

**A1.** **Do you agree to have your computer screen recorded:**

Yes ☒

No □

**A2.** **Do you consent to participate in this research study?**

Yes ☒

No □

**A3.** **Signature of participant:**

Ethan Leider

**A4.** **Date:**

05/05/2020