*Written and Research by:* JustinC. Erardo

*Submitted to:*

**Wyndham Central College**

101 Shaws Rd, Werribee VIC 3030

# Blowing the Cover: Experimental Study on the Vulnerability of Teenagers to Trojan Horse Malware

**IMMO:**Advanced Security Development Research

>SIMPLE DEFENS

### Abstract

Its no surprise that Millions of individuals worldwide had been affected by malicious software referred to as Trojan Horse viruses. These types of computer viruses typically hide themselves as innocent files until either manually opened and executed by the victim or automatically executes itself as soon as it has reached the host device wherein it does its thing. Trojan horses are typically hard to detect, but usually they can be detectable with little knowledge. The purpose of this study is to determine the capability of the students and how vulnerable the students are to Trojan Malware. The researcher was then able to collect significant data from the volunteered subjects gathered from [selected environment]. Insights were formulated from the experiment and provided that [summarized conclusion].

### Acknowledgement

The study would like to recognize the cooperation of Wyndham Central College Authorized Personnel/Staff and its Students in making the study possible with its participation heavily contributing to directing the course of the whole research. The whole educational paper would not be possible with the help of the Researcher and their helper/contributors, and the past studies which provided the existing information the researcher needed to widen the ideas throughout the study.

### Definition of Terms

* Anti-virus - A type of program that specializes in detection, prevention, and elimination of known Malware.
* Computer - any gadget/device capable of computing power
* Cybersecurity - A branch of Information Technology that focuses on the security of networks of computers.
* ILOVEYOU Virus - 2000’s email loveletter virus deemed ‘The most dangerous virus in the world’.
* Malware - a Malicious software or program.
* Population - referring to the group of participants.
* Trojan Horse - a type of malware that uses a disguise.
* Visual Basic Script(VBS) - a type of visual basic file that specializes on computer control and management.

## Chapter I. The Problem and Background

This chapter presents the introduction to the study, statement of the problem, theoretical background, research flowchart, scope and limitations, and the significance of the study.

**Introduction**

The use of technology and the internet today is becoming more and more common, with the existence of online communicagtion and tools to help individuals make their day to day life much easier. But with the rise of dependence to technology, comes with the risks found in the cyberworld. As the world becomes more and more online, the emergence of cybersecurity threats like malware has become a major concern for individuals, organzations and wide communities. One form of malware is a trojan horse; It is a type of computer virus that disguises itself as a legitimate-looking or harmless file or program; The malware got its name from the Aeneid by Virgil and Odyssey by Homer wherein the city of Troy were invaded by their enemies through the use of a wooden horse statue(Fortinet, n.d.). A 2022 statistical data states that the Trojan Horse Malware has contributed to 64.31% of cybersecurity attacks than most types of malware (Dekker, 2022). According to a report by the Internet Society, younger generations are more susceptible to such threats as they are the biggest users of the internet, and are more likely to engage in behaviors deemed 'risky' such as clicking on suspicious links or downloading files or programs from unknown sources; Additionally younger people have less experience and limited or currently developing knowledge on cybersecurity and how to protect themselves online.

The Following Research will serve as a guide on understanding the problem with trojan horse malware and the security of teenagers, expanding the knowledge on Trojan Horse Malware, its risks, and an overview of the experiment to determine the vulnerability of teenagers to Trojan Horse Malware; Provided also is the insights and conclusion regarding the conducted study on the selected participants on te experimentation. The study will also present the recommendation, a prototype to mitigate and protect the users from Trojan Horse Malware.

**Statement of the Problem**

The study focuses on the vulnerability of young ages 13 to 18 of Wyndham Central College Students which represents the age group of teenagers who are more susceptible to being victims of Trojan Horse Malware attacks. Specifically, still considering the age group, the experimental study aims to determine the following:

* What age is the most vulnerable?
* How easy is it for the students to fall victim to the attack?
* How aware are the students of trojan horse malware?
* How can the students and responsible adults mitigate and prevent trojan horse malware attacks

**Theoretical Framework**

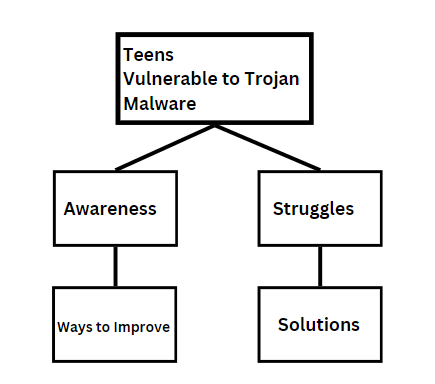


Figure 1.1 shows that the problem being Teenagers’ vulnerability to trojan horse leading to two things: Awareness, or how aware teenagers are of this, and Struggles, what occuring problems they may face from it, which leads to Ways to improve the Awareness and Solution, in order to mitigate, and prevent such attacks from reaching the teenagers.

**Scope and Delimitation**

The following study focuses on developing a universal solution to mitigate the problem, through an experimental study which involves determining the level of vulnerability between the age group of teenagers. The main participants of the study are Teenagers, specifically students aged 14-18 years old from Wyndham Central College S.Y. 2024. The researcher will gather insights through the use of online questionnaires with a target participant count of 100 students to determine and justify the vulnerability and awareness level of students which will be used to create an effective solution that will best suite them, as well as the people.

*Limitations*

The following limitations for the study include the willingness of students to partake in the experimental study, will affect the needed requirements to justify the research and the effectiveness of the proposed solution as it needs as much data as possible to meet the expectations and needs of the beneficiaries. Another limitation faced is the lack of related knowledge in order to widen the idea of the research. Since there are not many published papers regarding the research topic, the researcher will have difficulty in searching for available additional knowledge to further support the research.

**Significance of the Study**

The following research will benefit most personal computer systems and networks to eliminate and prevent Trojan malware attacks from occurring. The educational paper will therefore serve as a reference to increase the awareness of teenagers and responsible adults for their children about the dangers and will benefit from the solution.

The following beneficiaries of the research include:

**Teenagers and Parents**- The study will provide awareness and a prevention tool which then can be used to protect their personal computer systems from the Trojan Malware and the damage it delivers. As well as for parents to help their children do so.

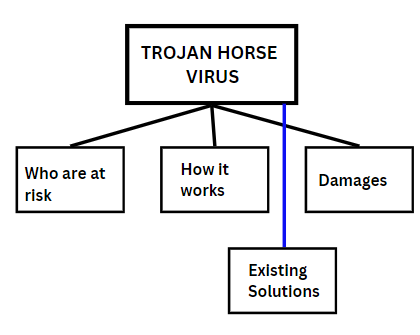
**Authorities and Experts** - the following study provides a recommendation for the suggested authorities such as cybersecurity departments of important institutions to improve the security of its networks and computer systems to prevent further damages.

**Future Researchers** - The study will serve as a reference for the future researchers to better understand the concepts and relations of Trojan horses to the generations of teenagers and how to increase awareness, prevent, and eliminate such malware.

## Chapter II Review of Related Literature and Studies

This chapter presents the concept map of the ideas in the study, and the review of related literature to further expand the understanding about the problem and existing solutions to support the study.

**Concept Map**



*Figure 1.2* indicates the following ideas needed for the understanding of this study. The following literature involve: Who are at risk of Trojan Horse Malware, how Trojan Horse Malware works, and the damages it costs to small of big computer network systems. There is as well provided the Existing solutions available used and are currently being used to prevent Trojan Horse Malware attacks.

**Who are at most risk from Trojan Attacks?**

According to citation(date), Windows Computers, includes those who use it, are the most common targets for Trojan Horse Malware attacks as it currently holds the biggest market share in the Operating System industry.

While age-specific wise, teenagers are more susceptible to these attacks as teens are the largest population to be online and using the internet than adults. (The internet society)

**How does a Trojan Horse Malware Work?**

According to Wijayarathne, Senesh(2022) in his case study report, a trojan virus, unlike most computer viruses, do not appear by itself. A Trojan Horse Malware infects a computer system when an individual downloads it from the server-side source of the program/application.

But for the malware to work, it states that the implementation of the executable (.exe), android package(.apk), or the iOS Installation Package(.ipa) must be installed on the device. So when the Program which is actually a Trojan Horse Malware gets installed, it infiltrates the system immediately, and activates whenever the infected computer device is on.

**Damages Done**

According to Statistic Data provided by *Worth Insurance(2023)*, Trojan horse malware have contributed to 58% of malware attacks globally. And an article from EFTSure(2022) states that 64.31% of malware attacks on windows systems come from Trojans; With over 788 million Trojan horse programs were detected by the cybersecurity company Avira. The ILOVEYOU Virus for instance have contributed to $8.7billion worth of damage during the 2000’s(Jovanovic, 2023).

**Existing Solutions**

A research study done by Zhefang, Zhu(2015), a few prevention measures were provided against the Trojan Horse Malware.

This includesPrevention in daily surfing process: 1. Never download and operate programs with ease, 2. Never open emails with ease, 3. Not downloading any programs sent by friends[As stated they may not be safe], 4. Never browse any suspicious websites, 5. Be civilized or careful when surfing on the internet. Also includes here Prevention by Computer Configurations: 1. Installing Antivirus Chip into the computer, 2. Use of Bootable and Repair Disks, 3. Use of Antivirus Software, 4. Installing a security patch program, 5. Shutdown[May prevent further damage if infected, Windows OS may save and recover some files through sudden shutdown but no guarantee of repair]. Lastly a recommendation on prevention through enhancing management of Computer networks: 1. Increase awareness amongst the population, 2. Enhance Legal Education in this field andthrough the broad cybersecurity, 3. Strengthen legislation to legally call to responsibility of Computer virus producers and transmitters and educate them.

**Relationship of the RRLS to the Study**

The following provided literature are needed to expand the understanding about the problem and to use the preexisting recommendations by past studies and the researchers to inspire the generation and development of an effective solution to aid in mitigating the problem of Trojan Horse Malware attacks on the vulnerable population.

## Chapter III Methodology

This chapter describes the research methodology and preparation fundamentals before carrying out the experimentation. The chapter provides the Research concept design, the research environment, research sampling methods, research participants, data gathering procedure, research instruments, and data analysis procedure.

**Research Design**

The following study focuses on the social-experimental approach, which uses two variables in an experiment to measure and obtain data. In this case an experiment following a student and various types of Harmless Trojan Horse virus will be received by the target. The test will measure how vulnerable and aware each age group in the teenage spectrum are in terms of various trojan horse malware.

**Research Environment**

The following study was conducted in the on-campus [computer laboratory] inside Wyndham Central College. The campus is located at 101 Shaws Rd., Werribee VIC 3030, host to more than 1300 students.

The following educational institution is fit into the study as a secondary provides the perfect age group to be selected to participate.

**Research Sampling**

For this study, Quota sampling method was used in gathering research participants. According to Nikolopoulou (2023), Quota sampling is a type of non-probability sampling which relies on dividing a group of participants into subgroups until a amount limit is met, hence named ‘quota’. In the experiment, an age range of 14-18 years old were selected to partake, each divided into two subgroups and each subgroup is grouped by their year level as a level of understanding. The criteria for selecting target participants include (i)Is a student from Wyndham Secondary College(ii)about 17 students from each year level from the school is needed(iii)Must have atleast basic awareness or background knowledge on the problem or the cybersecurity topic.

**Research Participants**

Following the Research sampling method used in the study and the criteria proposed by the researcher, 100 target participants were selected from Wyndham Central College, divided into 16 to 17 participants from each year level grouped as a standard for different levels of understanding. The age of participants ranged from 14 to 18 years old selected from year 7 to year 12.

**Research Instruments**

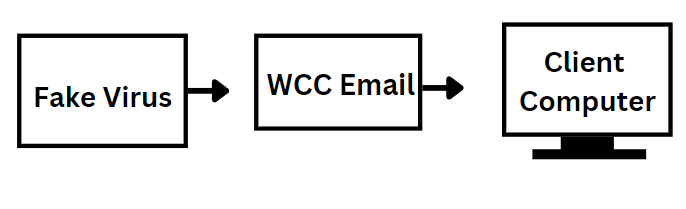
To test and determine the awareness of the participant in order to partake in the main experiment, they were asked through a simple online questionnaire. The questionnaire includes questions such as:

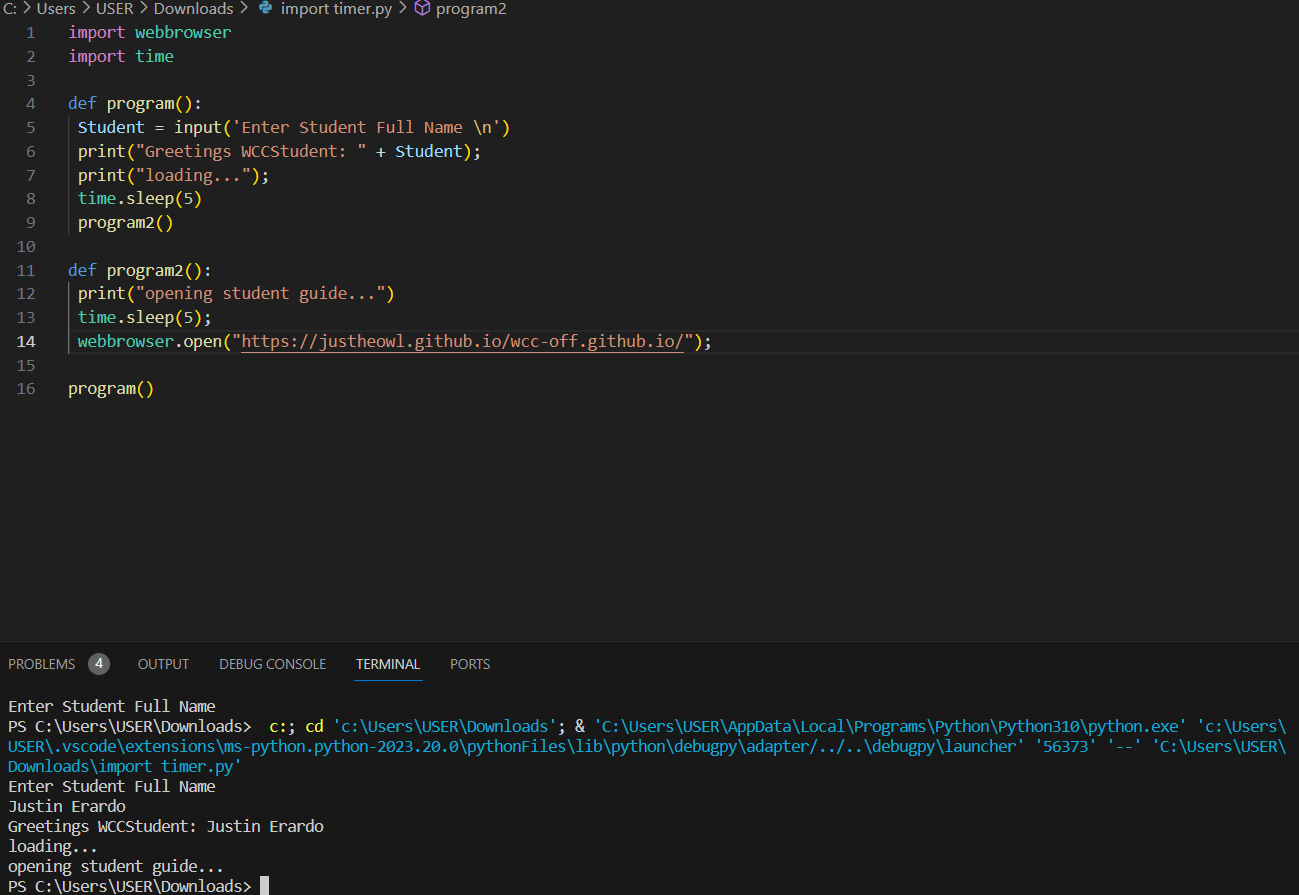
* In a range of 1 - 5 How are you likely to download any programs/apps from unknown sources (example third party apk installation sites)
* From 1-5, how likely would you open any unknown emails
* Given this situation: Your friend sent you an installation package (exe, apk, ipa) without telling you anything about the file, would you download it? (y/n)

Notes: The questionnaire would be both a per-experiment questionnaire and a post-experiment synthesis questionnaire.

*Social Experiment Procedure*

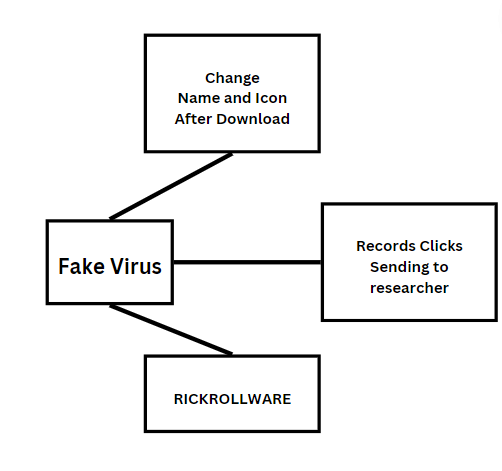
The following experiment procedure involves the participant being called by a personnel cooperating with the researcher to make the social experiment possible. The set up is done in the Computer lab and the participant will be asked to open their email. After signing in, the participant is expected to receive an email specifically sent to him, avoiding other contacts to be visible via CC to prevent ruining the experiment. The email contained a greeting from the school and file which the student will be asked to install. Through keen observation, the participant is expected to think thoroughly and observe any suspicious activity within the email; If the participant decides to ignore any red flags, and proceeds to download the file and opens it, the program will execute.

*Figure 1.3* Shows how the process of the experiment will work. The Fake Virus will come in an attachement that will be sent by the email distributor used by the school to be distributed to the email of a student. This social experiment involves the student being called out to fill in a form in which he has to download a “file”.

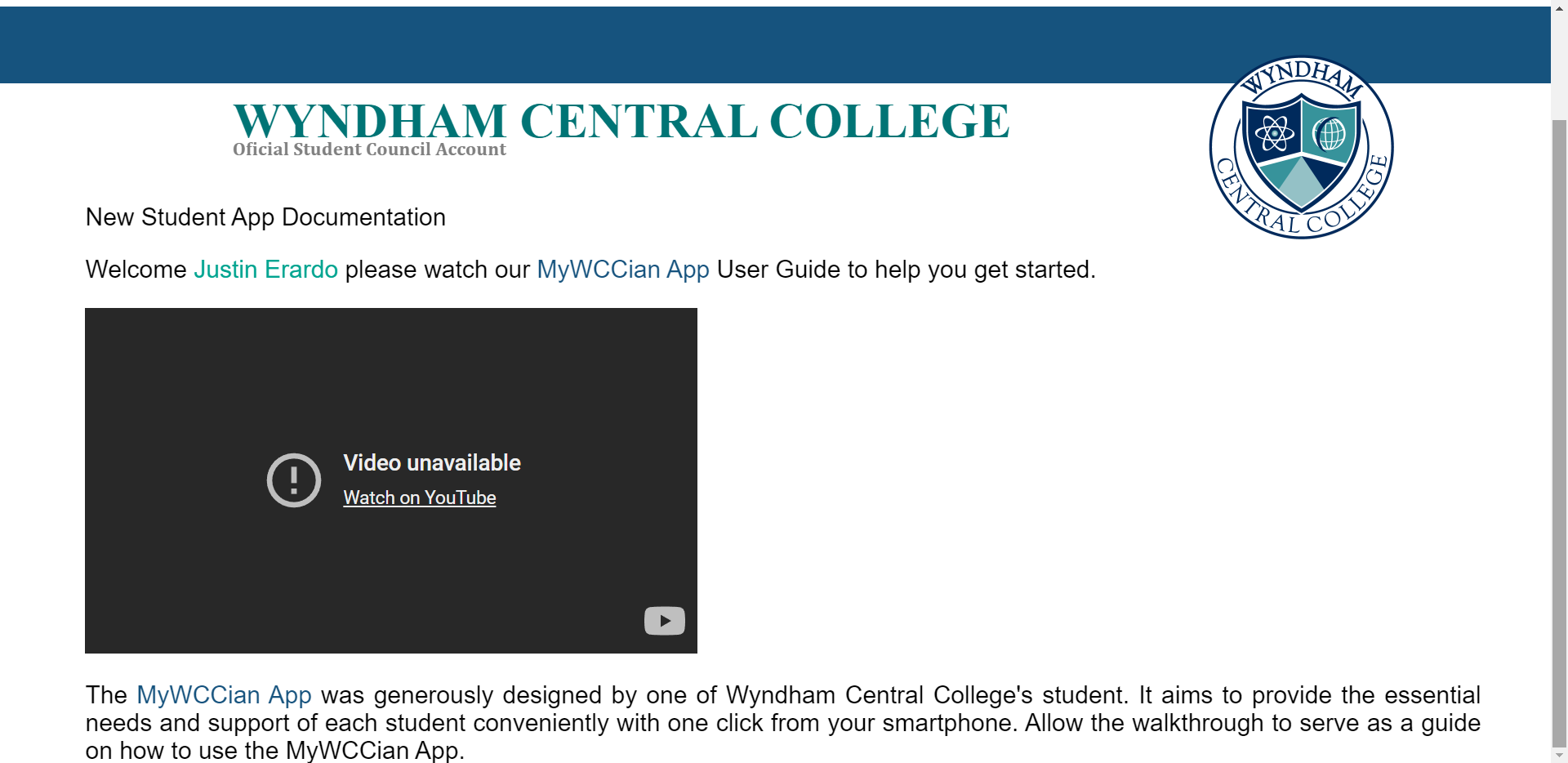


*Figure 1.4* Shows the outline or the code of the experiment program. The Program’s purpose is a harmless virus that only redirects the victim to a fake website created solely for the purpose of this experiment.

After the session, the participant will go through post-experiment assessment to gather data and personal insights to be used.



*Figure 1.5* describes what the experiment prototype is able to do. The prototype is designed to look and act like a real trojan, rather instead of being a real threat, it only possess the capability to ‘rickroll’ the subject.

Figure 1.6 shows the website included in the prototype.

**Data Gathering Procedure**The following pre-experiment questionnaires were sent through electronic mail in the Wyndham Central College Email database to be sent throughout hundreds of students. Those who will be selected will partake in the main experiment.

Through the experiment, the participants will be slightly monitored for any observations. After the experiment, the participants will be asked for insights and will be taken note of. The amount of participants who fell victim for the Trojan virus will be recorded as well through a remote database to keep on records to those who downloaded the file and the amount of times the video “Never gonna give you up - Rick Astley” was opened in the browser.

**Data Analysis Procedure**

Through an Online pre-experiment and post-experiment questionnaire, the Researcher was able to identify the awareness level, changes, and insights from the participants. Adding to this, the records noted from the experiment will determine the first research question of the study. With this, The researcher used organizational tools such as Excel, and Microsoft word to encode and sort the gathered data from the conducted study. Next the researcher identified all needed data to justify the conclusion and what will be needed to formulate and support the development of an effective recommendation.

## Chapter IV Analysis and Presentation of Data

This chapter proudly presents and describes the following discoveries, results, and insights from the data gathered after the successful experiment conducted by the researcher. Provided here is the detailed analysis, presentation of data, as well as the summary of findings.

1. Experimental Findings: Population Demographics
2. Experimental Findings: Observations and Results
3. Experimental Findings: Further Insights
4. Experimental Findings: Researcher Notes
5. Synthesis: Summary of Study

**To be continued after Chapter 3. See Webpage for Full Research Paper.**