

## TABLE OF CONTENTS

|   |      |
|---|------|
| UNDERGRADUATE THESIS PROPOSAL .....             | I    |
| APPROVAL PAGE .....                             | II   |
| ABSTRACT .....                                  | III  |
| TABLE OF CONTENTS .....                         | VII  |
| LIST OF FIGURES .....                           | X    |
| LIST OF TABLES .....                            | XII  |
| LIST OF EQUATIONS .....                         | XIII |
| CHAPTER I .....                                 | 14   |
| INTRODUCTION .....                              | 14   |
| 1.1 Research Background.....                    | 14   |
| 1.2 Research Problem.....                       | 15   |
| 1.3 Research Scope .....                        | 15   |
| 1.4 Research Objective .....                    | 16   |
| 1.5 Research Advantage.....                     | 16   |
| 1.6 Writing System.....                         | 16   |
| CHAPTER II.....                                 | 19   |
| LITERATURE REVIEW.....                          | 19   |
| 2.1 General Overview of Literature Review ..... | 19   |
| 2.2 Literature Review Comparison .....          | 20   |
| 2.3 Literature Review Conclusion.....           | 23   |
| CHAPTER III .....                               | 25   |
| THEORETICAL BASIS .....                         | 25   |
| 3.1 TLS Background.....                         | 25   |
| 3.2 Encrypted ClientHello Extension.....        | 28   |
| 3.3 Wireshark Packet Analysis tool.....         | 31   |
| 3.4 Oracle Virtualbox .....                     | 33   |
| 3.5 Openssl .....                               | 34   |
| 3.6 Curl.....                                   | 34   |
| 3.7 Nginx.....                                  | 35   |
| 3.8 Evaluation Metric.....                      | 35   |
| 3.8.1 Defining the Data Point .....             | 36   |

|  |    |
|--|----|
| 3.8.2 Descriptive Statistics .....                       | 36 |
| 3.8.3 Visualizations .....                               | 39 |
| 3.8.4 Inferential Statistics: .....                      | 40 |
| 3.9 Python.....  | 47 |
| CHAPTER IV .....   | 49 |
| RESEARCH METHODOLOGY .....                               | 49 |
| 4.1 Research Description.....                            | 49 |
| 4.2 Testbed Overview .....                               | 50 |
| 4.2.1 Server-side setup .....                            | 51 |
| 4.2.2 Client-Side Setup.....                             | 51 |
| 4.3 Data Acquisition.....                                | 52 |
| 4.3.1 Data Collection Preparation .....                  | 52 |
| 4.3.2 Packet Capture and Data Extraction.....            | 52 |
| 4.4 Data Analysis.....                                   | 53 |
| 4.4.1 Data Preparation.....                              | 53 |
| 4.4.2 Descriptive Statistics .....                       | 53 |
| 4.4.3 Visualization Techniques .....                     | 54 |
| 4.4.4 Inferential Statistics.....                        | 55 |
| CHAPTER V.....   | 58 |
| RESEARCH IMPLEMENTATION .....                            | 58 |
| 5.1 Testbed Setup .....                                  | 58 |
| 5.2 Server-Side Configuration .....                      | 61 |
| 5.2.1 Cloning the ECH Repository .....                   | 61 |
| 5.2.2 Generating TLS Certificates and ECH key-pair ..... | 62 |
| 5.2.3 Nginx Configuration.....                           | 62 |
| 5.3 Client-Side Configuration.....                       | 65 |
| 5.3.1 Building ECH-enabled cURL.....                     | 65 |
| 5.3.2 Wireshark Set up .....                             | 66 |
| 5.4 Data Acquisition.....                                | 66 |
| 5.4.1 Data Acquisition Preparation .....                 | 66 |
| 5.4.2 Packet Capture and Data Extraction.....            | 70 |
| CHAPTER VI .....   | 73 |
| RESULTS & ANALYSIS .....                                 | 73 |
| 6.1 Data Preparation .....                               | 73 |

|  |     |
|--|-----|
| 6.2 Statistical Analysis.....                        | 80  |
| 6.2.1 Descriptive Statistics Procedures .....        | 80  |
| 6.2.2 Visualization Methods .....                    | 81  |
| 6.2.3 Inferential Statistics Techniques.....         | 84  |
| 6.3 Results .....                                    | 89  |
| 6.3.1 Descriptive Statistics.....                    | 89  |
| 6.3.2 Visualization .....                            | 89  |
| 6.3.3 Inferential Statistics.....                    | 95  |
| 6.4 Discussion and Comparative Analysis.....         | 96  |
| 6.4.1 Analysis of Descriptive Statistics .....       | 96  |
| 6.4.2 Visualization Insights.....                    | 97  |
| 6.4.3 Interpretation of Inferential Statistics ..... | 97  |
| 6.5 Comparison with existing Literatures.....        | 98  |
| 6.6 Limitations.....                                 | 99  |
| 6.7 Practical Implications.....                      | 100 |
| 6.7.1 Enhanced User Experience .....                 | 100 |
| 6.7.2 Business Value .....                           | 100 |
| 6.7.3 Recommendations for Implementation .....       | 101 |
| 6.8 Summary of Findings.....                         | 101 |
| CHAPTER VII.....                                     | 104 |
| CONCLUSION & SUGGESTIONS.....                        | 104 |
| 7.1 Conclusion.....                                  | 104 |
| 7.2 Suggestions .....                                | 105 |
| REFERENCES.....                                      | 106 |