**Appendix A**

**Proposal Cover**

|  |
| --- |
| **PROPOSAL**  IMAGE STEGANOGRAPHY SYSTEM  IZZAT AQIL MOHAMED  012019070938  DIPLOMA IN COMPUTER FORENSICS  MANAGEMENT AND SCIENCE UNIVERSITY |
| For office use only (Leave this blank)    Approved Rejected    Approved with changes  Comments:  Evaluated by:  Name:  Date: |

**Appendix B**

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **TABLE OF CONTENTS** | | |
| CHAPTER | | **Page** |
| I | INTRODUCTION   * 1. Project background   2. Problem statement   3. Objectives of the project   4. Scope of the project   5. Significance of the project   6. Limitation of the project   7. Summary | 1  1  2  3  4  5  6  7 |
| II | LITERATURE REVIEW   * 1. Review of Current Situation   2. Review of Related Products      1. Crypture      2. rSteg      3. SSuite Picsel   3. Comparison Table | 8  8  9  9  10  11  12 |
| III | METHODOLOGY   * 1. Project Methodology   2. Hardware and Software requirement   3. Project Schedule   4. ERD   5. DFD   6. User Interface Design | 13  13  16  17  18  18  19 |
| IV  V | CONCLUSION  4.1 Conclusion  4.2 Print Interface  4.3 Questionnaire Survey  5.1 Conclusion | 20  20  21  22  24 |
|  |  |  |

**CHAPTER 1: INTRODUCTION**

**1.1 Project Background**

Since the rise of the internet the majority of our communication has been done through it since it is a transformative technology that allows us to connect to different parts of the world as one global virtual world. People are able to overcome the wall that is distance and freely communicate and exchange information. However, this brings about a new problem and a major one which is the security of information. This is particularly important in the case of confidential data.

Cryptography is widely known and has been developed over the years all for one goal to provide secrecy of communication by changing data into a form eavesdropper cannot understand. Even though this is an amazing way of providing secrecy of communication it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message a secret. This is where steganography comes into play.

Redundant media are known for being used for steganography since those digital media are capable of change without any possibility to detect the alteration. Image and audio files satisfy this requirement particularly well. In fact, digital images are the most used carrier file formats owing to their popularity on the internet. For example, in a 2018 article written by The Wall Street Journal, every morning in India people send by the masses “Good Morning” images to their friends and families to the point that Facebook servers which host the WhatsApp text messenger can freeze up. With the number of images going around every day image steganography becomes a very powerful technique to be utilized by those who put importance on security and privacy.

**1.2 Problem Statement**

1. The prevalent and persistent data leaks done by black hats.

* The number of data leaks occurring in Malaysia that happened throughout the years are eye opening. Unfortunately, even services that are handled by companies outside of Malaysia are getting hacked left and right, like the recent Uber case. No one seems to be out of grasps since recently even the Malaysia prime minister got his Telegram account hacked.

1. Limited privacy from the prying eyes of big corporations.

* In our current world it is unavoidable that everyone has to use services from at least one of the big corporations in the world for example Meta. These companies are known from previous cases to track and monitor their users’ activities for revenue.

1. Relay of information.

* Since there is very limited privacy and security once something has been uploaded to the internet some sensitive cases like police work or company secrets are at a vulnerable position and such makes it hard to work when doubt is present.

**1.3 Objectives**

1. To create a system for which users can mask and unmask messages that are hidden behind an image through steganography.
2. To provide users of the system additional layer of safety and privacy when sending a message through the internet.

**1.4 Scope of The Project**

1. **User Scope**

User is able to open a received image in the system and show the hidden message or input an image of their own and input their own message to the image and save it to their pc folder.

1. **System Scope**

* Open Image

Opens the users folders for them to choose an image to insert into the system.

* Show Data

When an image is inserted, there is an option to show data which makes the system read the hidden message embedded by another user.

* Hide Data

After inserting a picture there will be text box where the user can write their message to embed. Press the hide data button and the data will be embedded unto the picture.

* Save Image

Images that have been embedded a message can be saved to the users computer folder using this button.

**1.5 Significance of The Project**

With the significant increase in data leaks be it in this country or globally, people stand the risk of losing their privacy at any moment since hackers are always finding a way to disrupt the big tech corporations. The people must take measures to defend themselves against such mishap so that in any trouble occurred they do not affect the peoples physical or digital information. This system acts as another added layer of privacy to anyone who might use it. Exchange information through imagery while may not be as robust as encryption or hashing it is deceptive in nature so as unsuspecting hackers that get a hold of users’ data may overlook it.

A lot is at stake, people’s data are regularly being sold on the internet. This system helps the people regain their privacy from potential data leaks or even corporations that sell your data for profit. Using image steganography if a leak happens your logs are not obvious on first sight and requires digging by the attacker which most would not do since they are handling a large amount of data at one moment. This protects the people from having their information floating around the web such as their home address or anything private to one’s life.

**1.6 Limitation of The Project**

* Image Size

The system can only accept images up to a limit. Images in the bigger sizes cannot be used by the system or may not work as intended.

* Text Limit

Text that can be imbued unto the image has a limited number of words. To send longer information users may need to be crafty and send a few images.

* Security

While this system is to add a level of privacy it doesn’t have much of security. Any person who may check the image on the steganography system may see the imbued message.

* Desktop Reliant

This system is built for desktop use only and is not be readily available on a smartphone where most communication occurs.

**1.7 Summary**

Project background discusses regarding the reason for going through with this project as well as methods created and used in the industry regarding attaining privacy in communication. Problem statement is the problems that are affecting people daily that we are trying to fix with this system. The objectives discuss on the goals of creating this system and what it will focus on. Scope of the project will be the range of motion on what a user and the system can do. The significance of the project talks about the benefits and empowerment that may affect users lives. Lastly, limitations elaborate on what limitations this system will face even when completed.

**CHAPTER 2: LITERATURE REVIEW**

**2.1 Review current situation**

We are seeing a huge uprising in data breaches across the globe. In recent memory, huge companies/platforms such as Twitch and Uber had been breached and had their users information sold and leaked on the internet. These breaches are not uncommon and may already be affecting the average person. A study conducted by cybersecurity company Surfshark has placed Malaysia as the 11th most breached country in the second quarter of 2022 which is an astounding growth of 733% in the last quarter. In a recent case, allegedly it is found that National Registration Department (NRD) has had a data breach which contained information of 22.5 million Malaysians born between 1940 and 2004. This data breach contained the information of 22.5 million peoples full name, IC numbers, addresses and photographs. The three most used social media or chatting platform in Malaysia is WhatsApp, Facebook and Instagram. While some of these have chat encryption it doesn’t hurt to up the privacy level for using such platform for information transfers. The purpose of this work is to increase the level of privacy for any person who might find a use for it. This is one way to prevent such life altering information being sold raw on the internet. Even if it might not reduce the amount of data breaches happening in this country it might just protect information that some people hold dear.

* 1. **Review of Related Products**

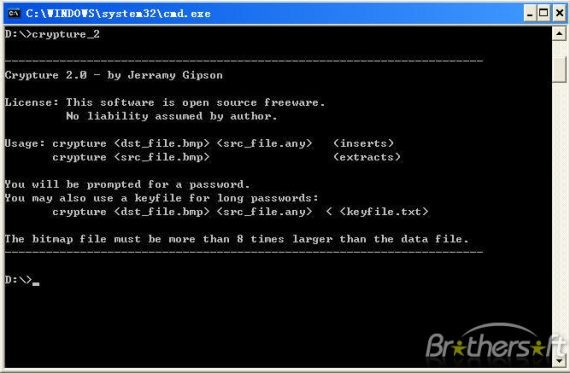


Figure 2.1: Crypture

Crypture uses command line interface to perform Steganography. Using Crypture, you can hide your sensitive data using BMP images files. But there is one requirement for this Steganography to happen. The Image file should be 8 times larger than the data file, which you want to encrypt. Crypture is only 6KB in size and it doesn’t need any installation.

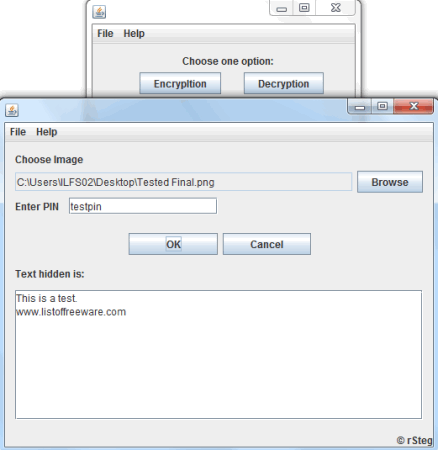


Figure 2.2: rSteg

rSteg is yet another Steganography tool developed using Java. You need to have Java installed on your machine to run rSteg. Another striking advantage is its portable feature. Hence no need to install it, just run and the software windows pop up. Performing Steganography using rSteg is simple. You need an Image file, text to be encrypted and password to be set for decryption. The final output is stored as PNG. Plug the image into the same Steganography detection tool for decryption along with a password.



Figure 2.3: SSuite Picsel

SSuite Picsel is a free portable application to hide text inside an image file. However, it has a different approach. It uses the image file as a key to protect your hidden text inside an image. Don’t be confused. Actually, this tool can hide text inside an image file. Nevertheless, to hide and reveal text inside an image, you need to enter another image as a key. To hide text inside the image, select the image in which you want to hide the text and select another image for the key. Now you can hide your text inside the first image. To reveal the text, you need to enter the key image.

* 1. **Comparison Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **System Features** | **Crypture** | **rSteg** | **SSuite Picsel** | **Image Steganography System** |
| **Password Required** | NO | YES | YES | YES |
| **Lightweight Size** | YES | YES | YES | YES |
| **Require Third Party Software** | NO | YES | NO | NO |
| **Can**  **Decrypt** | NO | YES | YES | YES |

**CHAPTER 3: METHODOLOGY**

**3.1 Project Methodology**

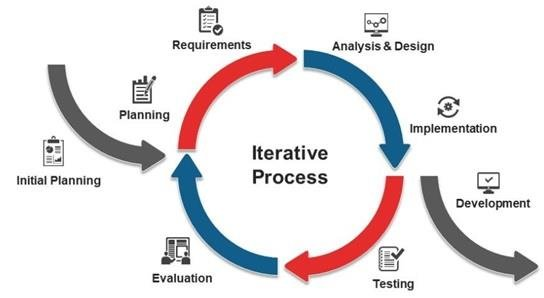
****

Figure 3.1.2 Iterative Model

This SDLC model emphasizes repetition. Developers create a version very quickly and for relatively little cost, then test and improve it through rapid and successive versions.

Using the iterative model methodology, I can leave tiny details that may stop the workflow at the start and focus on creating a working product first then when the product is usable, I can then start to add features that I had left before. This way I can avert my focus towards more productive workflow as I am not stressing over one feature that may not help the completion of the application.

**Planning**

The goal of the first phase which is planning is to scope out the problems of the system beforehand so that you may find a solution which should take into consideration the costs of resources and time.

**Requirements**

This second phase is where I start to think of functional requirements that are required of the project and its solutions. This is all to ensure the expectations of the system is met.

Analysis & Design

Here in this phase is the time to properly set in stone the necessary specifications, operations and features that will contribute towards the completion and success of the application.

**Development**

I start developing from what I have and start the process of creating a working product.

**Testing**

This phase focuses in system testing to determine if the system design works with what has been lay out before in the earlier phases.

**Evaluation**

Following the iterative model in this phase an evaluation is done for the test product and is sent back to planning as to further improve on the semi-finished system.

**Implementation**

After multiple repeats and evaluation and fixes only then will the system be implemented.

**3.2 Hardware and Software Requirement**

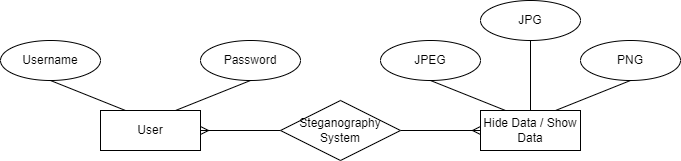
|  |  |
| --- | --- |
| **Hardware** | **Requirements** |
| **PC** | **Intel i3**  **8GB RAM**  **500GB HDD** |

|  |  |
| --- | --- |
| **Software** | **Requirement** |
| Operating System | Windows 10 |
| Coding Tools | Python |
| Development Support Tools | PIP / IDLE |
| Browser | Google Chrome |

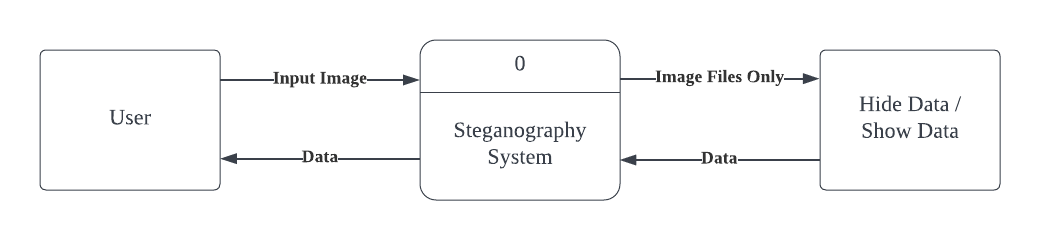
**3.3 Project Schedule: Gantt Chart**

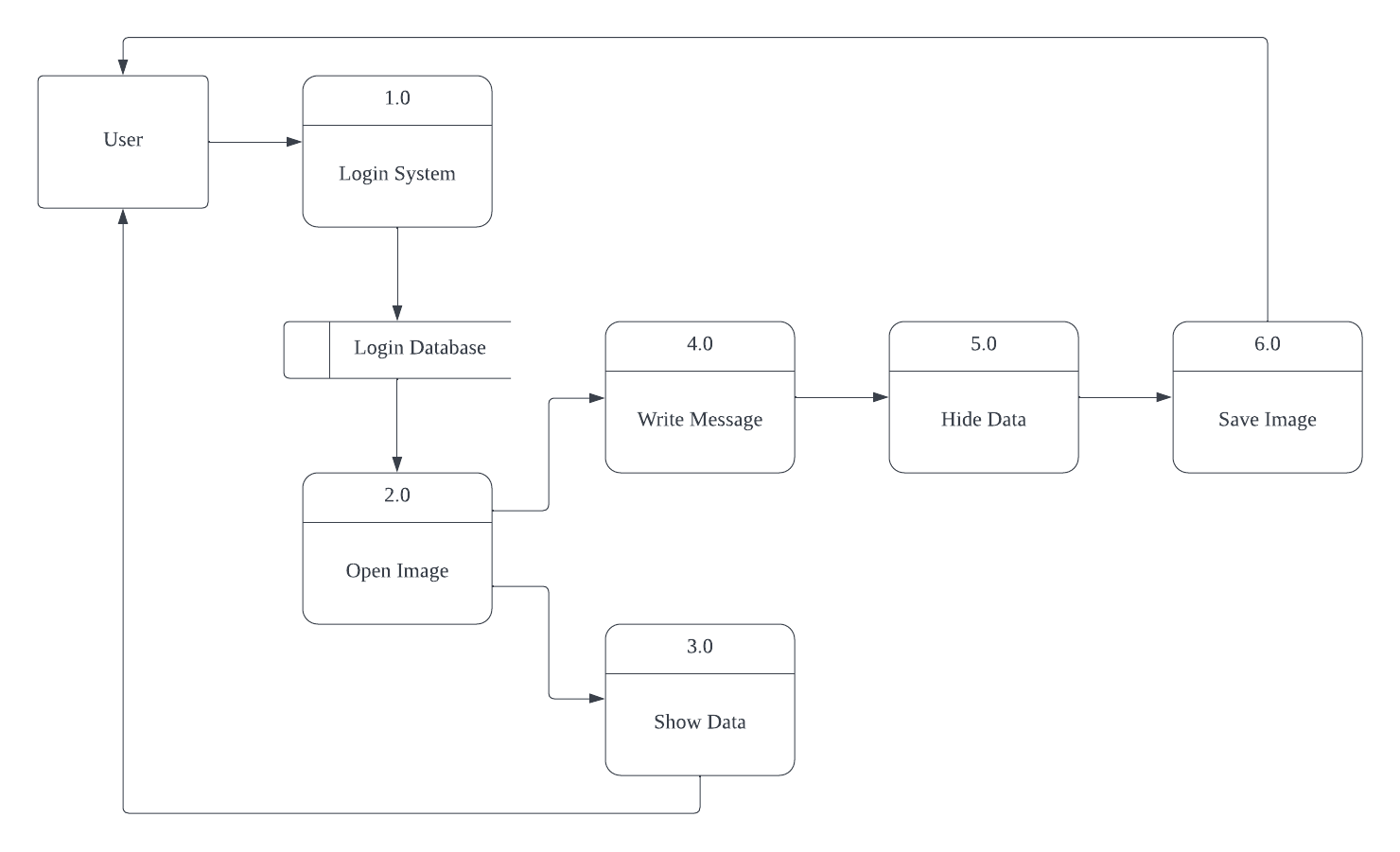
****

**3.4 ERD**



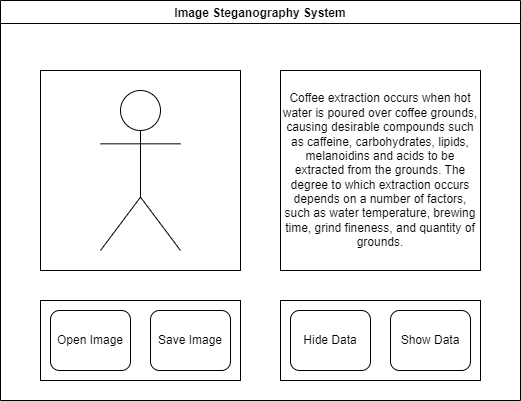
**3.5 DFD**





**3.6 User Interface Design**



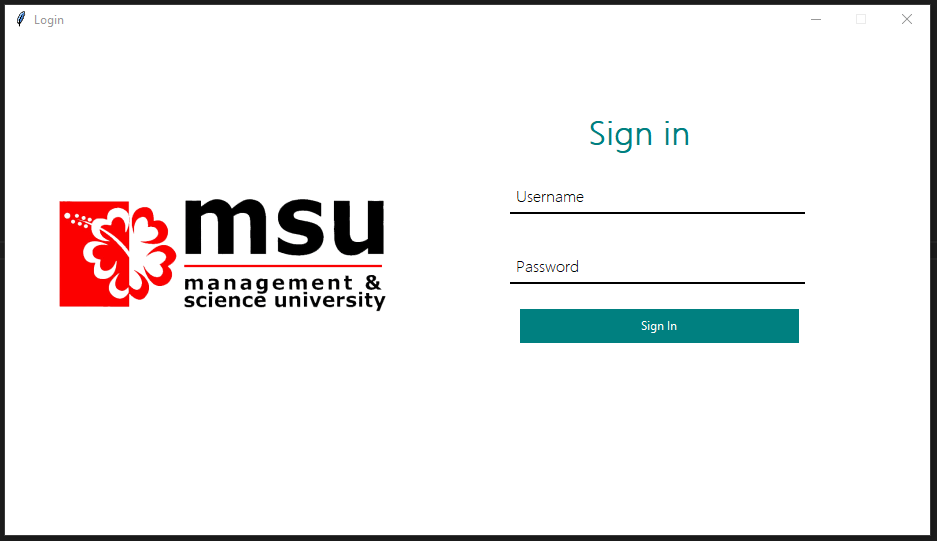


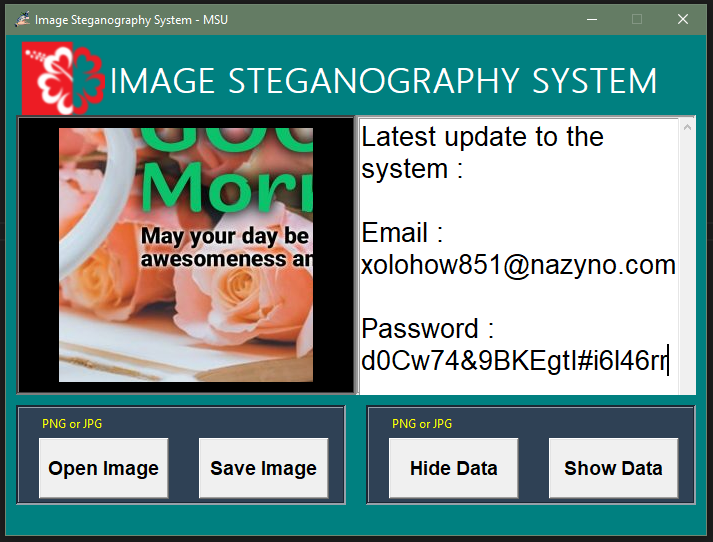
**CHAPTER 4: CONCLUSION**

**4.1 Conclusion**

The Image Steganography System will be developed on the Python platform which will serve as the main foundation of the system. After rigorous thought has been given towards the benefits and disadvantages of the system and how it may impact casual everyday people who communicate through the internet, the system will finally be developed and tested. This project aims to elevate the quality of life for anyone who is privacy concerned or simply want to start adding privacy to their lives. This system will be focused on increasing the privacy of communication online therefore increase security of people who are not being singled out targeted by hackers. The resources that will be used to create this system will be at a minimum since it is being developed on Python and its tools which are largely open-source.

**4.2 Print Interface**





**4.3 Questionnaire Survey**

**CHAPTER 5**

**5.1 Conclusion**

The awareness among surveyed of the current situation may not be satisfactory but the mindset of protecting one's self and one’s privacy against such mishap is present. People largely do care for their own privacy and if there is a method to do so people are willing to incorporate it into their lives. The system created may not be bullet proof against a focused attacker but it will increase one’s security of transmitting information online and that is an important base to build upon. In an ideal world this privacy protection or increase level of information security is implemented and worked on at a higher level but since that is not the case individuals must take the step to protect themselves.

**Bibliography**

**Azmi, H. (2022, July 4). Why is Malaysia seeing a rise in data leaks, and what is the government doing to stop it?. South China Morning Post.** [**https://www.scmp.com/week-asia/article/3183878/why-malaysia-seeing-rise-data-leaks-and-what-government-doing-stop-it**](https://www.scmp.com/week-asia/article/3183878/why-malaysia-seeing-rise-data-leaks-and-what-government-doing-stop-it)

**Reporters, F. (2022, May 23). Disclose data leak probe findings, govt urged. Free Malaysia Today.** [**https://www.freemalaysiatoday.com/category/nation/2022/05/23/disclose-data-leak-probe-findings-govt-urged/**](https://www.freemalaysiatoday.com/category/nation/2022/05/23/disclose-data-leak-probe-findings-govt-urged/)

**Team, B. (2022, July 20). #TECH: Malaysia is #11 in most breached country list for Q2 2022 – study. New Straits Time.**

[**https://www.nst.com.my/lifestyle/bots/2022/07/815021/tech-malaysia-11-most-breached-country-list-q2-2022-study**](https://www.nst.com.my/lifestyle/bots/2022/07/815021/tech-malaysia-11-most-breached-country-list-q2-2022-study)

**Markets, T. E. (2021, August 24). 73% of Malaysian organisations expect data breach that impacts customer data in next 12 months — Trend Micro. The Edge Markets.** [**https://www.theedgemarkets.com/article/73-malaysian-organisations-expect-data-breach-impacts-customer-data-next-12-months-%E2%80%94-trend**](https://www.theedgemarkets.com/article/73-malaysian-organisations-expect-data-breach-impacts-customer-data-next-12-months-%E2%80%94-trend)

**Asia, C. I. (2022, July 26). ② Social Media Penetration in Malaysia [Research]. Digital Business Lab.** [**https://digital-business-lab.com/2022/07/%E2%91%A1-social-media-penetration-in-malaysia-research/**](https://digital-business-lab.com/2022/07/%E2%91%A1-social-media-penetration-in-malaysia-research/)

**Yadav, P. (2022, Dec 5). Another cybersecurity firm alleges WhatsApp data leak after denial by messaging app. CNBC.** [**https://www.cnbctv18.com/technology/another-cybersecurity-firm-alleges-whatsapp-data-leak-15329791.htm**](https://www.cnbctv18.com/technology/another-cybersecurity-firm-alleges-whatsapp-data-leak-15329791.htm)