A white circle with black text

Description automatically generated

PHISHING CAMPAIGN FOR VICTORIA POLICE

By AHP Private Limited

ANAGHA P- 223709844 & HUDSON PETERS -221025058

TABLE OF CONTENTS

INTRODUCTION 2

General Introduction 2

Target Audiences 2

Database Design Objectives 2

Database Design Benefits 2

Assumptions 3

Attributes and Business Rules 3

DATABASE DESIGNS 6

Database 1: Voter Turnouts and Voting Results 6

Master Table 6

1NF Table 6

2NF Table 7

3NF Table 9

Database 2: Candidate Details with Voting Updates 11

Master Table 11

1NF Table 12

2NF Table 13

3NF Table 14

Database 3: Public Opinion Poll 16

Master Table 16

1NF Table 16

2NF Table 17

3NF Table 18

REFERENCES 19

### General Introduction

This report explores phishing campaigns targeting law enforcement, with a focus on the Victorian Police Department. It aims to analyse the cybersecurity challenges these agencies face, emphasizing ethical considerations and the broader implications for global law enforcement. The report serves as an educational resource to enhance understanding and responses to such digital threats.

### Target Audiences

* **Database 1: Phishing Campaign manager**
* **Database 2: Police department (User)**
* **Database 3: HR manager**

### Database Design Objectives

**Database 1**: The objective is to automate the analysis of a phishing simulation on the Victorian Police Department, targeting specific personnel groups with tailored emails linked to dummy phishing sites. Variables include campaign details, target audience behaviour, and response metrics. The goal is to identify security awareness levels and automate reporting for targeted cyber defence improvements.

**Database 2:**   
The database design objectives for this dataset aim to structure personnel information and interaction with a cybersecurity initiative in a multi-table format. It normalizes officer details (OfficerID, FirstName, LastName, Department, Rank, BadgeNumber, Region, Suburb, Gender, HireDate, BirthDate, Email), campaign interaction (Opened Emails, Clicked Emails, Opened Email Attachment, Reported Using PhishHook), and rank descriptions into separate 2NF tables to remove partial dependencies. The 3NF further refines relationships by correlating officers to departments and badges, ensuring all attributes depend directly on the primary key for streamlined data management and query efficiency.

**Database 3**: **Analytical:** To analyse phishing defence within the Victorian Police Department by correlating officer training status, compliance, incident response, and campaign feedback, thereby identifying targeted areas for cybersecurity enhancement.

**Automation Objective:** To design an automated solution that compiles phishing campaign data, evaluates departmental readiness, and produces comprehensive reports on campaign impact and officer engagement, streamlining the process for continuous security posture assessment.

Top of Form

### Database Design Benefits

**Database 1:** The design enhances the Victorian Police Department's cybersecurity by automating the analysis of training efficacy and compliance. It provides strategic insights into phishing campaign effectiveness and officer satisfaction, enabling targeted improvements and resource optimization, thereby boosting overall security preparedness and personnel engagement.

**Database 2:** Normalization reduces data redundancy, ensuring consistency in personnel and department records. The design allows easy updating of individual records without affecting others, minimizing data entry errors.

Separation into 2NF and 3NF tables facilitates complex queries for reporting and analytics, supporting effective decision-making.

Efficient data structure streamlines the process of tracking officer interactions with cybersecurity campaigns.

**Database 3:** The design streamlines data analysis, providing actionable insights into phishing susceptibility and training effectiveness. It automates feedback collection and compliance tracking, enabling prompt identification of security gaps and facilitating data-driven decisions to bolster the Victorian Police Department's cyber defences.

### Assumptions

**Database 1:**

* Uniformed officers showed the highest email opening rate at 85%, which may suggest a high level of engagement or possibly a greater susceptibility to phishing attempts due to their frequent communication via email.
* The 60% click-through rate for the emails targeted at uniformed officers indicates a significant interaction with the phishing content, implying a potential gap in awareness or training effectiveness that requires further investigation.
* Detectives and investigators had a 70% rate of using the PhishHook response tool, reflecting a high level of vigilance or effective training in recognizing phishing attempts amongst this group.
* The absence of clicked email percentages for IT and Cybersecurity Personnel, along with Administrative Staff, suggests a need for additional data to fully assess the phishing campaign's impact on these groups.
* IT and Cybersecurity Personnel showed an 80% success rate for an unstated metric, possibly indicating robust protocols or inherent scepticism towards phishing, considering their professional focus on security.
* The targeted phishing campaign revealed varying levels of policy compliance verification across departments, pointing to the need for tailored approaches in future security protocol updates and training programs.

**Database 2:**

* In 1NF, uniformed officers, having the highest email open rate, may suggest that their data, once duplicated across tables, now indicates potential vulnerabilities or high engagement, due to the unique entry for each interaction.
* The dataset in 2NF, by separating officer information from interaction data, allows us to assume that targeted training may be needed, as evidenced by the differentiated click-through rates for dispatchers versus detectives.
* With 3NF, assuming transitive dependencies have been removed, we might infer that PhishHook reporting is an independent action from email interaction, hence the varying response rates across departments could signal different levels of phishing threat awareness.
* The absence of interaction data (click rates) for IT and Cybersecurity personnel suggests they may not be the primary targets, or their awareness is sufficiently high, hence not engaging with the phishing attempt, which aligns with their professional focus.
* The varying levels of compliance across departments highlighted in 2NF tables assume that customized approaches in protocol updates could be more effective.
* Considering the structured design in 3NF, we can assume that departmental feedback and satisfaction ratings are directly associated with campaign IDs, offering a direct measure of campaign impact for refined future strategies.

**Database 3:**

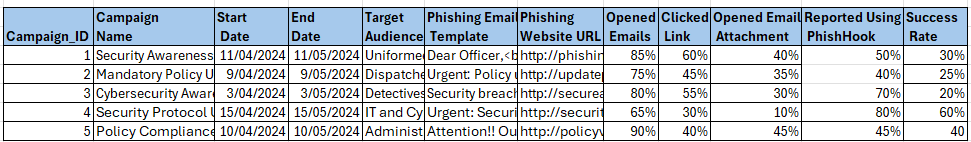
* The dataset's 1NF representation implies that each phishing campaign is uniquely identified, targeting specific roles within the Victorian Police Department, such as Uniformed Officers and IT Personnel.
* The progression to 2NF suggests that the dataset includes specific interaction metrics like emails opened and clicked, which could indicate the effectiveness of the phishing campaign's targeting and content.
* High open rates among Uniformed Officers might point to either a lack of email vigilance or a need for more robust phishing awareness training.
* Disparities in Clicked Emails and Success Rates across roles hint at differential susceptibility to phishing, warranting customized training interventions.
* The utilization of 3NF structures indicates that feedback on the phishing campaign is systematically captured to facilitate a clear understanding of departmental feedback and the need for awareness training.
* A notable Phish Hook response rate, particularly among Detectives and Investigators, could reflect a heightened awareness or more effective training methodologies within these groups.
* The absence of click rate data for IT and Cybersecurity Personnel may either indicate a high level of security awareness or a gap in the dataset that requires attention.
* The dataset's normalization suggests a meticulous approach to organizing phishing simulation data to optimize cybersecurity measures.

**Attributes and Business Rules:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute** | **Data Type** | **Description** | **Business Rule** |
| Campaign\_ID | Integer | Unique identifier for each phishing campaign | Must be a unique integer; primary key |
| Campaign Name | Varchar | Descriptive name of the phishing campaign | Cannot be null; descriptive text |
| Start Date | Date | Date when the phishing campaign begins | Must be on or before the End Date |
| End Date | Date | Date when the phishing campaign ends | Must be on or after the Start Date |
| Target Audience | Varchar | Group within the police department targeted by the campaign | Must correspond to an existing department group |
| Phishing Email Template | Varchar | The template text for the phishing email | Should follow predefined structure for simulations |
| Phishing Website URL | Varchar | The web address for the phishing simulation | Should be a valid URL format |
| Open Rate | Decimal | The ratio of recipients who opened the email | Between 0 and 1, or 0 to 100% when displayed |
| Click Rate | Decimal | The ratio of recipients who clicked a link in the email | Between 0 and 1, or 0 to 100% when displayed |
| Submission Rate | Decimal | The ratio of recipients who submitted data on the phishing site | Between 0 and 1, or 0 to 100% when displayed |
| Success Rate | Decimal | The ratio of targeted phishing attempts that succeeded | Between 0 and 1, or 0 to 100% when displayed |
| Status | Varchar | The current state of the phishing campaign | Should be a valid status such as 'Active', 'Inactive', or 'Completed' |
| Officer ID | Integer | Unique identifier for each officer. | Must be unique and not null. Primary key for the Officer entity. |
| First name | Varchar | Officer's given name. | Must be a text string, not null. |
| Last name | Varchar | Officer's family name. | Must be a text string, not null. |
| Department | Varchar | Department where the officer works. | Must correspond to an existing department within the police department, not null. |
| Rank | Varchar | Rank of the officer. | Must correspond to a predefined list of officer ranks, not null. |
| RankDescription | Varchar | Description of the officer's rank. | Textual description of the rank, can be null. |
| BadgeNumber | Integer | Unique identification number assigned to the officer. | Must be unique for each officer, not null. |
| Region | Varchar | Region where the officer is located. | Must be a valid region of operation, can be null. |
| Suburb | Varchar | Suburb within the region where the officer is located. | Must be a valid suburb within the region, can be null. |
| Gender | Char | Gender of the officer. | Must be 'M' for male or 'F' for female, not null. |
| HireDate | Date | Date when the officer was hired. | Must be a valid date in the past, not null. |
| BirthDate | Date | Officer's date of birth. | Must be a valid date, not null. |
| Email | Varchar | Officer's email address. | Must be a valid email format, not null. |
| Opened Emails | Boolean | Indicates if the officer opened phishing emails. | Must be 'true' if opened, 'false' if not, not null. |
| Clicked Emails | Boolean | Indicates if the officer clicked on links in phishing emails. | Must be 'true' if clicked, 'false' if not, not null. |
| Opened Email Attachment | Boolean | Indicates if the officer opened attachments in phishing emails. | Must be 'true' if attachment opened, 'false' if not, can be null. |
| Reported Using PhishHook | Boolean | Indicates if the officer reported phishing attempts using PhishHook. | Must be 'true' if reported using PhishHook, 'false' if not, not null. |
| OfficerID | Integer | Unique identifier for each officer in the police department. | Must be unique for each officer. Non-negative integer. |
| Department | Varchar | The department where the officer is assigned, such as Uniformed Officers, Dispatchers, etc. | Must be a valid department within the police department. Non-null. Categorical. |
| Officer training record | Varchar | Record of the phishing training status of the officer. | Can be 'Completed', 'In Progress', or 'Not Applicable'. Non-null. Categorical. |
| Officer compliance status | Varchar | Compliance status of the officer with the phishing training policy. | Can be 'Compliant' or 'Non-Compliant'. Non-null. Categorical. |
| Reported using PhishHook | Boolean | Indicates if the officer reported phishing using the PhishHook system. | Can be true (Yes) or false (No). Non-null. |
| Phishing incident response | Varchar | Status of the response to the phishing incident. | Can be 'Investigation ongoing', Non-null. Categorical. |
| Campaign ID | Integer | Identifier for the specific phishing campaign. | Must correspond to an existing campaign. Non-null. |
| Campaign effectiveness metrics | Varchar | Metrics used to measure the effectiveness of the phishing campaign. | Based on campaign goals, such as 'Improved click rates'etc. Non-null. Categorical. |
| Policy compliance verification | Varchar | Status of verification for policy compliance. | Can be 'Verified' or 'Non-verified'. Non-null. Categorical. |
| Officer feedback and awareness | Varchar | Feedback from officers regarding the phishing campaign and their awareness. | Open text for feedback; 'No feedback received' if nothing is provided. Can be null. |
| Campaign satisfaction rating | Numeric(2,1) | Rating given by officers for the satisfaction with the campaign on a scale of 1 to 10. | From 1 to 10, can be null if no rating is provided. |

**Database 1:**

**1NF**

****

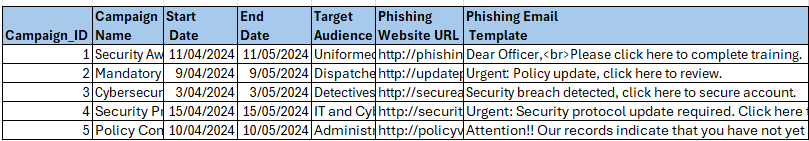
The database is designed in adherence to the First Normal Form (1NF) to facilitate the analysis of phishing campaign data within the police department. Applying 1NF ensures that each record is unique and there are no repeating groups, making the data suitable for digital processing. Attributes such as Campaign ID, Campaign Name, Start and End Dates, Target Audience, Phishing Email Template, and Phishing Website URL are singularly represented, providing a clear, unambiguous view of each campaign's parameters. Metrics like Opened Emails, Clicked Emails, Opened Email Attachment, Reported Using Phish Alert, and Success Rate are captured individually against each campaign, allowing for precise assessment of the effectiveness of phishing awareness strategies and pinpointing areas for improvement in cybersecurity training across various police department divisions. The 1NF structure lays the groundwork for reliable data manipulation and straightforward querying, which is crucial for analysing and enhancing phishing defence mechanisms.

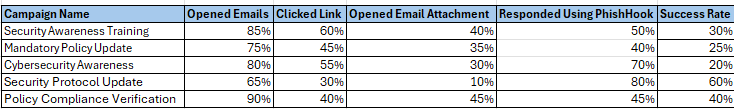
**Dependency Diagram Table 1.1**

**A close-up of a document

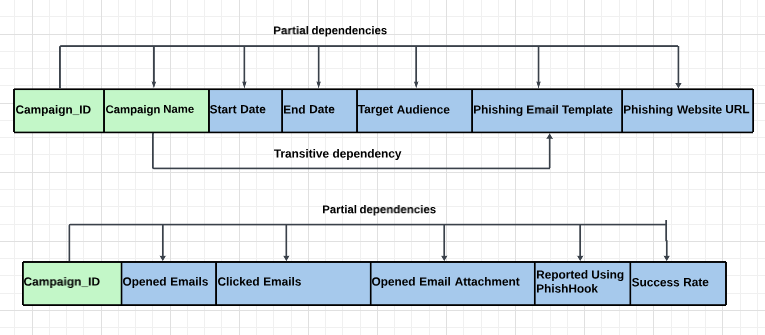
Description automatically generated**

**2NF**

****



In this refined 2NF database design, we use two linked tables to eliminate partial dependencies and clarify relationships. The first table uses 'Campaign ID' as the primary key, uniquely identifying each phishing campaign's attributes—'Campaign Name,' 'Start Date,' 'End Date,' 'Target Audience,' 'Phishing Website URL,' and 'Phishing Email Template.' The second table links 'Target Audience' with their interaction metrics—'Opened Emails,' 'Clicked Emails,' 'Opened Email Attachment,' 'Responded Using Phish Hook,' and 'Success Rate'—using a composite key of 'Campaign ID' and 'Target Audience.' This structure ensures each attribute is fully functionally dependent on the primary key, enhancing data normalization and preventing duplication. This systematic approach is vital for accurately measuring the effectiveness of phishing simulations, providing clear data sets for evaluating and improving cybersecurity awareness across different police department divisions.

****

**3NF**

A blue box with black text

Description automatically generated

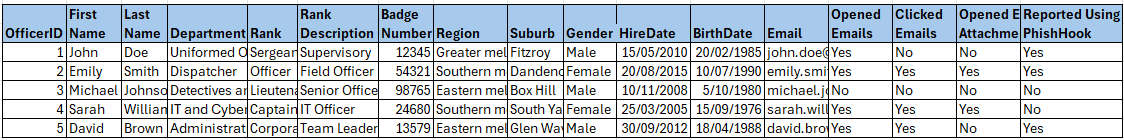
This dataset, organized in Third Normal Form (3NF), ensures that all attributes—'Campaign ID,' 'Campaign Name,' 'Start Date,' 'End Date,' 'Target Audience,' 'Phishing Email Template,' 'Phishing Website URL,' 'Opened Emails,' 'Clicked Emails,' 'Opened Email Attachment,' 'Responded Using Phish Hook,' and 'Success Rate'—are not only dependent on a primary key but also independent of each other. This eliminates transitive dependencies, facilitating targeted and efficient analysis of phishing campaign impact on distinct police department divisions.

**A diagram of email marketing

Description automatically generated**

**Database 2:**

**1NF**

****

This dataset is a comprehensive collection of data related to officers' interactions with a phishing simulation. Structured in 1NF, it includes individual records for each officer (OfficerID) with personal information (FirstName, LastName, Rank, RankDescription, BadgeNumber, Region, Suburb, Gender, HireDate, BirthDate, Email) and their specific responses to phishing attempts (Opened Emails, Clicked Emails, Opened Email Attachment, Reported Using PhishHook). Each field contains only atomic data, there are no repeating groups, and each entry is unique, facilitating precise tracking and analysis of the phishing campaign's effectiveness among various police department roles.

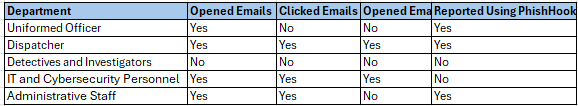
**Dependency Diagram Table 2**

A diagram of a computer program

Description automatically generated with medium confidence

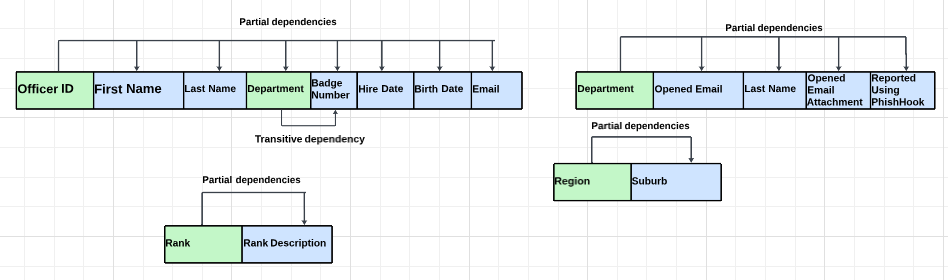
**2NF**

****

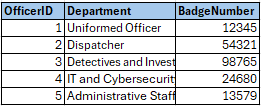
****

****

This dataset, in Second Normal Form (2NF), removes partial dependencies by segregating officer data and phishing interaction details. Each officer is identified by 'OfficerID', with personal information such as 'FirstName', 'LastName', 'Gender', 'Department', 'HireDate', 'BirthDate', 'Email', and 'BadgeNumber' detailed in one table. Separate tables capture department-specific phishing interactions ('Opened Emails', 'Clicked Emails', 'Opened Email Attachment', 'Reported Using PhishHook') and standardized departmental roles ('Rank', 'RankDescription'), as well as geographical locations ('Region', 'Suburb'). 2NF ensures relationships within these attributes relate directly to primary keys without redundancy.



**3NF**

****

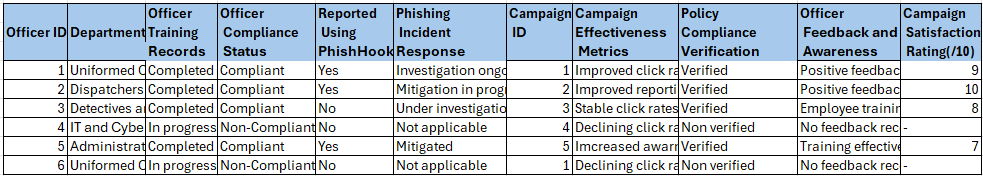
This dataset in Third Normal Form (3NF) ensures that each table contains only data that is directly related to the primary key, which in this case is 'OfficerID'. The attributes 'Department' and 'BadgeNumber' are functionally dependent only on 'OfficerID', removing transitive dependencies. This results in a table where each officer is associated with a single department and a unique badge number, facilitating accurate and efficient queries related to departmental assignments and officer identification within the organizational structure. The 3NF structure enhances data integrity and prevents anomalies in database operations.

**A diagram of a company structure

Description automatically generated**

**Database 3:**

**1NF**

****

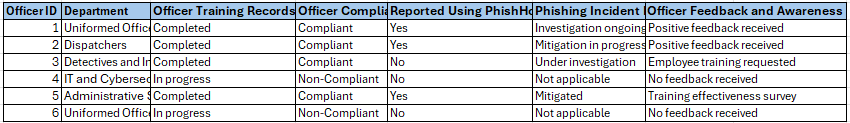
This dataset, organized in First Normal Form (1NF), contains records for police officers with attributes including 'Officer ID', 'Department', 'Officer Training Records', 'Officer Compliance Status', 'Reported Using Phish Hook', 'Phishing Incident Response', linked to specific 'Campaign ID'. Each 'Campaign ID' correlates with 'Campaign Effectiveness Metrics', 'Policy Compliance Verification', 'Officer Feedback and Awareness', and 'Campaign Satisfaction Rating'. The adherence to 1NF ensures that each entry is atomic, with no repeating groups, facilitating unambiguous data analysis for evaluating cybersecurity training outcomes and compliance within the police force.

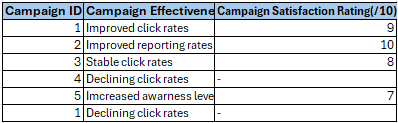
**Dependency Diagram Table 3**

**A screenshot of a computer

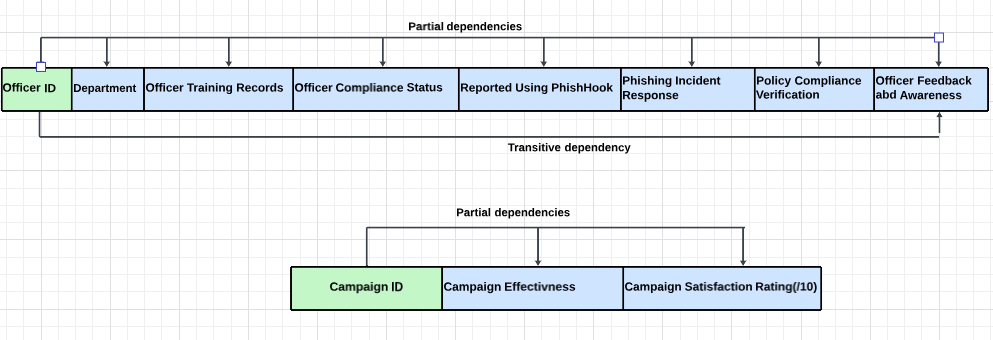
Description automatically generated**

**2NF**

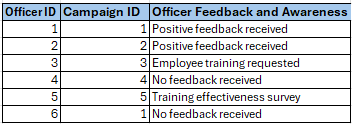
****

****

This 2NF dataset organizes officer-specific data and campaign results into separate tables to remove partial dependencies. Attributes like 'Officer ID', 'Department', 'Officer Training Records', 'Officer Compliance Status', 'Reported Using Phish Hook', 'Phishing Incident Response', and 'Officer Feedback and Awareness' are detailed for each officer, while 'Campaign ID', 'Campaign Effectiveness Metrics', and 'Campaign Satisfaction Rating' are documented per campaign. Each table's primary key (Officer ID and Campaign ID) ensures data is related but independent, eliminating duplication and enabling precise analysis of training impact and phishing campaign effectiveness within the police force.



**3NF**

****

In Third Normal Form (3NF), the dataset has attributes 'Officer ID', 'Campaign ID', and 'Officer Feedback and Awareness' to eliminate transitive dependencies and ensure that attributes are only dependent on the primary key. The 'Officer ID' and 'Campaign ID' serve as a composite key to uniquely associate officer feedback with the respective campaign. This organization enables clear and direct mapping of feedback to specific phishing campaigns, vital for analysing training effectiveness without the clutter of interdependent data, thereby optimizing the database for concise, non-redundant information storage and retrieval.

A diagram of a company

Description automatically generated

**REFERENCES**

JavaTPoint. (2011). DBMS Normalization - javatpoint. [Www.javatpoint.com](http://www.javatpoint.com/). <https://www.javatpoint.com/dbms-normalization>

Lucidchart. (2023). Online diagram software & visual solution | Lucidchart. Lucidchart. <https://www.lucidchart.com/pages/>

*Working to keep our community safe*. (n.d.). Www.police.vic.gov.au. https://www.police.vic.gov.au/

**MIS781 – Business Intelligence and Database**

**Trimester 1, 2024**

**Group Assignment**

**GROUP MEMBER CONTRIBUTION FORM**

Group Number:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name (Print)** | **Student ID** | **%Contribution** | **Signature\*** |
| **1. Hudson Peters** | **221025058** | **50%** |  |
| **2. Anagha Prashanth Raje URS** | **223709844** | **50%** | **A signature on a white surface  Description automatically generated** |

**Note**: \* By signing here, I hereby declare that this is my original work.