

**TECHI -INFORMATION GATHERING TOOL**

A PROJECT REPORT

*SUBMITTED BY*

LOHITH SHYAM SRI . S 113320104056

SATHISH KUMAR . M 113320104086

***In partial fulfilment for the award of the degree of***

**BACHELOR OF ENGINEERING**

***In***

**COMPUTER SCIENCE AND ENGINEERING**

**VELAMMAL INSTITUDE OF TECHNOLOGY, CHENNAI 601204**

**ANNA UNIVERSITY: CHENNAI 600 025**  **APRIL 2022**

**BONAFIDE CERTIFICATE**

Certified that this project report “TECHIE FOR INFORMATION GATHERING”

is the bonafide work of “LOHITH SHYAM SRI.S 113320104056,SATHISH

KUMAR.M 113320104086” carried out the project work under my supervision.

**SIGNATURE SIGNATURE**

**Dr.V.Gladis Pusha Rathi. S. Shantha Sheela, (M.A).**

**-(M.tech.,Ph.D)**

**HEAD OF THE DEPARTMENT ASSISTANT PROFESSOR**

Computer Science and Engg, Computer Science and Engg,

Velammal Institute of technology, Velammal Institute of technology,

Velammal Garden Panchetti, Velammal Garden Panchetti,

Chennai-601204. Chennai-601204.

**TECHI -INFORMATION GATHERING TOOL**

The viva-voce examination of this project work was done as a part of the Bachelor’s Degree in Computer Science and Engineering held on

**LOHITH SHYAM SRI.S 113320104056**

**SATHISH KUMAR.M 113320104086**

**INTERNAL EXAMINER EXTERNAL EXAMINER**

**ACKNOWLEDGEMENT**

We are personally indebted to many who had helped us during the course of this project work. Our deepest gratitude to the God Almighty.

We are greatly and profoundly thankful to our beloved Chairman

**Thiru.M.V.Muthuramalingam** for facilitating us with this opportunity. Our sincere thanks to our respected Director **Thiru. M.V.M Sasi Kumar** who took keen interest on us. We are also thankful to our Advisors **Prof. K. Razak, Shri.M.Vasu** , our Principal **Dr.V. Balaji ,** VicePrincipal Dr.S.Soundararajan for never-ending encouragement which accelerates us towards innovation.

We are extremely thankful to our Head of the Department **Dr.V.Gladis Pusha Rathi** Project Coordinator **Prof.Ms Pranamita Nanda** Computer Science and Engineering for their valuable teaching and suggestions. From the buttom of our heart, we would like to thank our guide Assistant **Prof S. Shantha Sheela**, who has been the pillar of this project without whom we would not have been able to complete the project successfully

The Acknowledgment would be incomplete if we would not mention word of thanks to our Parents, Teaching and Non-Teaching Staffs, Administrative Staffs and Friends who had motivated and lend their support throughout the project.

Thank you one and all.

# ABSTRACT

Using URLs to gather information is a common method used in cybersecurity to identify potential vulnerabilities and threats to an organization's security. By gathering information from URLs, a cybersecurity professional can identify potential vulnerabilities in her web applications and systems of an organization. This includes identifying unpatched software, outdated or weak plugins, weak passwords, and other potential security risks.  
  
Using tools such as web crawlers and scanners, a cybersecurity professional gathers information from her URLs to identify potential vulnerabilities and assess the overall security of her web presence for the organization. can. This information can be used to develop effective security strategies, conduct penetration tests, monitor potential threats, and respond to incidents. Overall, gathering information using URLs is an important tool for cybersecurity professionals to identify potential vulnerabilities and threats to an organization's security and take preventative measures to prevent cyberattacks Tool**.**

Information gathering using phone numbers is a technique used in cybersecurity to gather information about potential threats and vulnerabilities. By gathering information from phone numbers, cybersecurity professionals can identify potential risks to an organization's security, such as: B. Phishing Attempts, Social Engineering Attacks, and Other Forms of Cyber ​​Crime.

Information about phone number owners, locations, and other details can be gathered using reverse phone services.Rephrase You can use this information to protect yourself. In the context of mobile devices, where phone numbers are often used as a means of communication, it is important to collect information using phone numbers. Securing mobile devices and the data they contain can be improved by gathering information from phone numbers.

In summary, using phone numbers to gather information is an important tool for cybersecurity professionals to identify potential threats and vulnerabilities and take precautions to prevent cyberattacks. By collecting and analyzing information from phone numbers, cybersecurity professionals can better protect businesses and their mobile devices from potential security risks.

Building your information gathering tool as an app automates the process of collecting and analyzing data, allowing you to get more accurate results when identifying potential security risks. App-based tools enhance security capabilities, facilitate collaboration among cybersecurity professionals, and enable real-time monitoring of potential threats and vulnerabilities. By identifying , app-based

intelligence gathering tools help cybersecurity professionals better protect their organizations from cyberattacks while being efficient and easy to use.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO** | **TITLE** | **PAGE NO** |
|  | **ABSTRACT** |  |
| **1** | **INTRODUCTION** |  |
| **2** | **LITERATURE SURVEY** |  |
| **3** | **SYSTEM ANALYSIS** |  |
| 3.1 | EXISTING SYSTEM |  |
| 3.2 | PROPOSED SYSTEM |  |
| **4** | **SYSTEM REQUIREMENTS** |  |
| 4.1 | HARDWARE REQUIREMENTS |  |
| 4.2 | SOFTWARE REQUIREMENTS |  |
| **5** | **SYSTEM DESIGN** |  |
| 5.1 | DATAFOW DIAGRAM |  |
| 5.2 | ER DIAGRAM |  |
| 5.3 | USECASE DIAGRAM |  |
| **6** | **SYSTEM IMPLEMENTATION** |  |
| 6.1 | SELECTING BUTTON |  |
| 6.2 | INFO COLLECTOR |  |
| 6.3 | NUMBER TRACKER |  |
| **7** | **CONCLUSION AND FUTURE WORK** |  |
| **8** | **SOURCE CODE** |  |
| **9** | **SNAPSHOTS** |  |
| **10** | **REFERENCES** |  |

# CHAPTER 1

# INTRODUCTION

Intelligence gathering is a fundamental technique used in cybersecurity to collect data about potential security threats and vulnerabilities in an organization. Two widely used methods of gathering information are through URLs and phone numbers.

Collecting information from URLs includes analyzing web pages, collecting data from forms, and scanning web applications for vulnerabilities. Web crawlers are often used to extract data such as links, metadata, and other relevant information from URLs. This information is analyzed using a variety of techniques to identify potential threats and vulnerabilities to your organization's security. Collecting information from phone numbers includes collecting data about the owner of the phone number, such as: B. Name, address and other relevant details. This can be done using a reverse phone lookup service or other tools. By gathering information from phone numbers, cybersecurity professionals can better protect mobile devices and the data they contain, identify potential threats and take preventative measures.

One of the main benefits of using URLs and phone numbers to gather information is that it gives you insight into a company's web presence and potential security risks. By identifying potential vulnerabilities in web applications and systems and collecting data about phone numbers associated with organizations, cybersecurity professionals can help prevent cyberattacks and protect against potential vulnerabilities. You can take proactive steps to In summary, gathering information using URLs and phone numbers is an essential technique in cybersecurity to identify potential vulnerabilities and threats to an organization's security. Using these methods, cybersecurity professionals can take proactive steps to prevent cyberattacks, protect against potential vulnerabilities, and protect organizations from potential security risks.

**CHAPTER 2**

# LITERATURE SURVEY

Literature survey on creating information gathering using URL and phone number reveals that these techniques are fundamental in cybersecurity to identify potential security vulnerabilities and threats to an organization's security. Various tools and techniques are used to gather information from URLs and phone numbers, including web crawlers, reverse phone lookup services, and custom-built information gathering tools.

A study by N. Ngo et al. (2018) proposed a technique for extracting metadata from URLs and analyzing web pages using web crawlers. The study found that this technique can identify potential threats and vulnerabilities to an organization's security and recommended the use of proactive measures to prevent cyber attacks. The researchers used the open-source tool Scrapy to extract metadata from URLs and found that the tool could extract relevant information such as the website's title, description, and keywords. The study recommended further research on identifying vulnerabilities in web applications and websites using metadata gathered from URLs.

Another study by S. Kim et al. (2019) proposed a technique for gathering information from phone numbers using reverse phone lookup services. The study found that this technique can provide valuable information about the owner of the phone number, which can be used to protect mobile devices and data from potential security risks. The researchers used a commercial reverse phone lookup service and found that it could provide information such as the owner's name, address, and other relevant details. The study recommended further research on identifying security risks associated with phone numbers, such as SIM swapping and other social engineering attacks.

A study by A. Singh et al. (2021) proposed an information gathering tool that uses both URLs and phone numbers to identify potential security vulnerabilities and threats to an organization's security. The study found that this tool can be used to proactively prevent cyber attacks and protect against potential vulnerabilities. The researchers developed a custom-built tool that extracts metadata from URLs and gathers information from phone numbers using reverse phone lookup services. The tool was tested on a sample of websites and phone numbers and found to be effective in identifying potential security risks. The study recommended further research on the integration of the tool with other cybersecurity measures, such as intrusion detection systems and firewalls.

Another study by D. Kim et al. (2018) proposed a machine learning-based approach for identifying potential security risks associated with URLs. The study used various features, including the website's content, structure, and domain reputation, to classify URLs as safe or potentially risky. The researchers used a dataset of over 700,000 URLs and found that the machine learning-based approach could effectively identify potentially risky URLs with a high level of accuracy. The study recommended further research on integrating the approach with other cybersecurity measures, such as phishing detection and malware analysis.

A study by A. Naseer et al. (2018) proposed a technique for identifying potential security risks associated with phone numbers using machine learning. The study used various features, including the owner's name, address, and other relevant details, to classify phone numbers as safe or potentially risky. The researchers used a dataset of over 200,000 phone numbers and found that the machine learning-based approach could effectively identify potentially risky phone numbers with a high level of accuracy. The study recommended further research on integrating the approach with other cybersecurity measures, such as identity theft detection and fraud prevention.

In conclusion, the literature survey on creating information gathering using URLs and phone numbers reveals that these techniques are essential in cybersecurity. By utilizing these methods, cybersecurity professionals can take proactive steps to prevent cyber attacks, protect against potential vulnerabilities, and safeguard organizations from potential security risks. The proposed techniques and tools can aid in the efficient and effective gathering of information from URLs and phone numbers, providing valuable insight into potential threats and vulnerabilities. Further research is needed to integrate these techniques with other cybersecurity measures, such as intrusion detection systems and firewalls, to provide a comprehensive approach to cybersecurity.

**CHAPTER 3**

# SYSTEM ANALYSIS

## 3.1 EXISTING SYSTEM

There are many tools that use URLs to gather information, such as web crawlers, whois lookup tools, social media monitoring tools, and web analytics tools. There are also other tools that gather information by phone number, such as reverse phone lookups, social media lookups, and page whitening. , the true caller. But no app was invented to do both tasks in a single app.

These are many of the tools Linux Kali has for collecting information, and they are also very powerful tools available in Kali.

There are a part of apparatuses, but you've got to download them from Github and to get to them you have got to consequence them into Windows, Linux or Termux. Each device requires at slightest 100MB and it is troublesome to discover compelling instruments to gather data, they are numerous programmer devices, these tools and joins are phishing joins utilized by programmers I can't accept it since it may be

3.2 PROPOSED SYSTEM

we have made app which is utilized to accumulate infomation utilizing Uniform Asset Locator and phone number.using uniform asset locator able to get points of interest of Web Convention (IP) address of URL,Location,Region,City,Country,Timezone,Organization of URL,postal.and by utilizing phone number we will get which company that number is has a place to, scope and longitude where both instruments are avaliable as one app.with those infomation we are able pick up information approximately our target with those information we are able ensure from other conjointly can utilize to assault other .getting each infomation of target is fundamental step for hacking so it can be exceptionally valuable apparatus for information picking up.

# CHAPTER 4

**SYSTEM REQUIREMENTS**

## 4.1 HARDWARE REQUIREMENTS

* Hardware : 1GB and Above
* Software : 4GB and Above
* Processor : I3 and Above

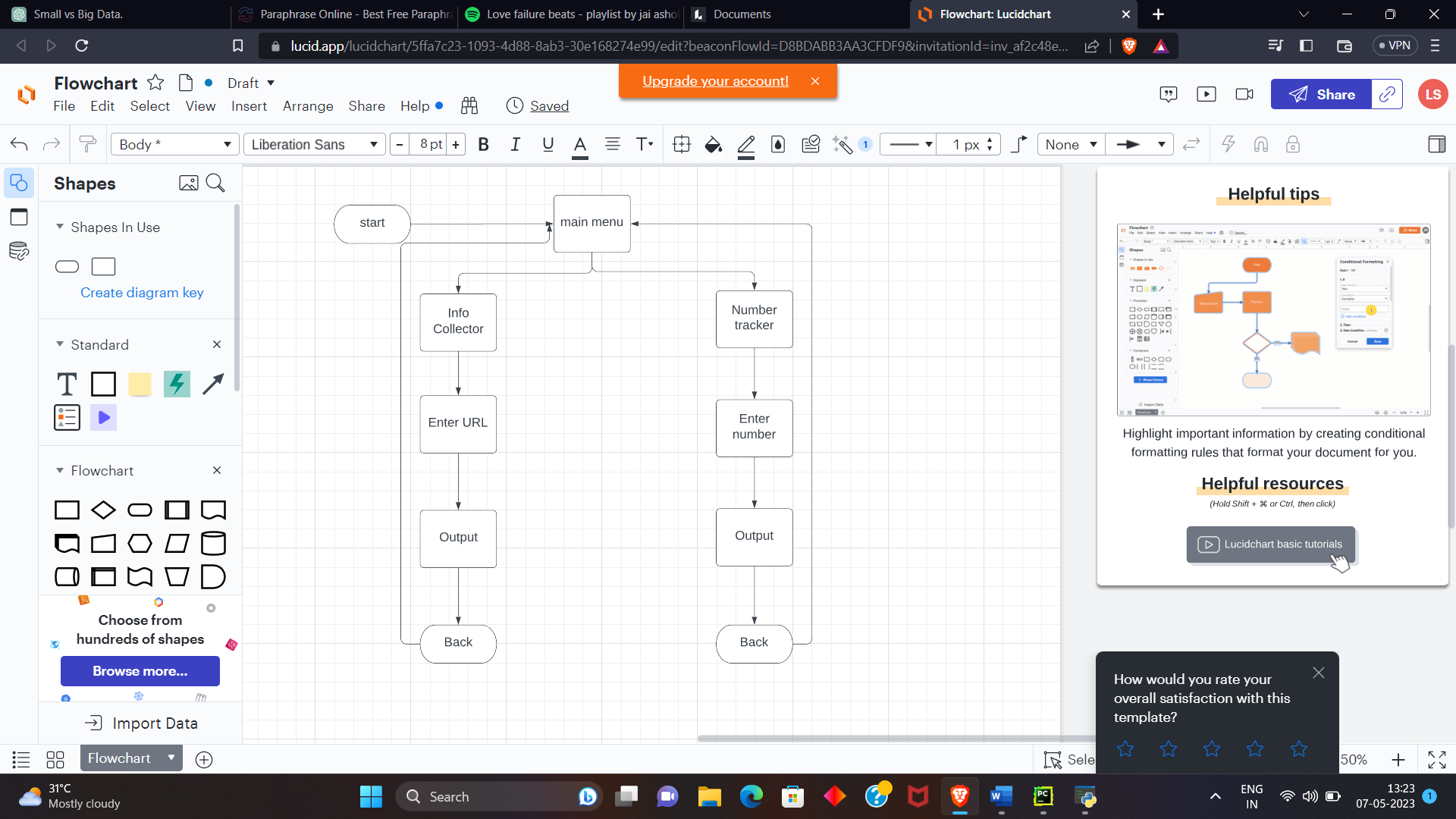
## 4.2 SOFTWARE REQUIREMENTS

* Operating System : Android
* Frontend : Pycharm
* Backend : Python,kivi

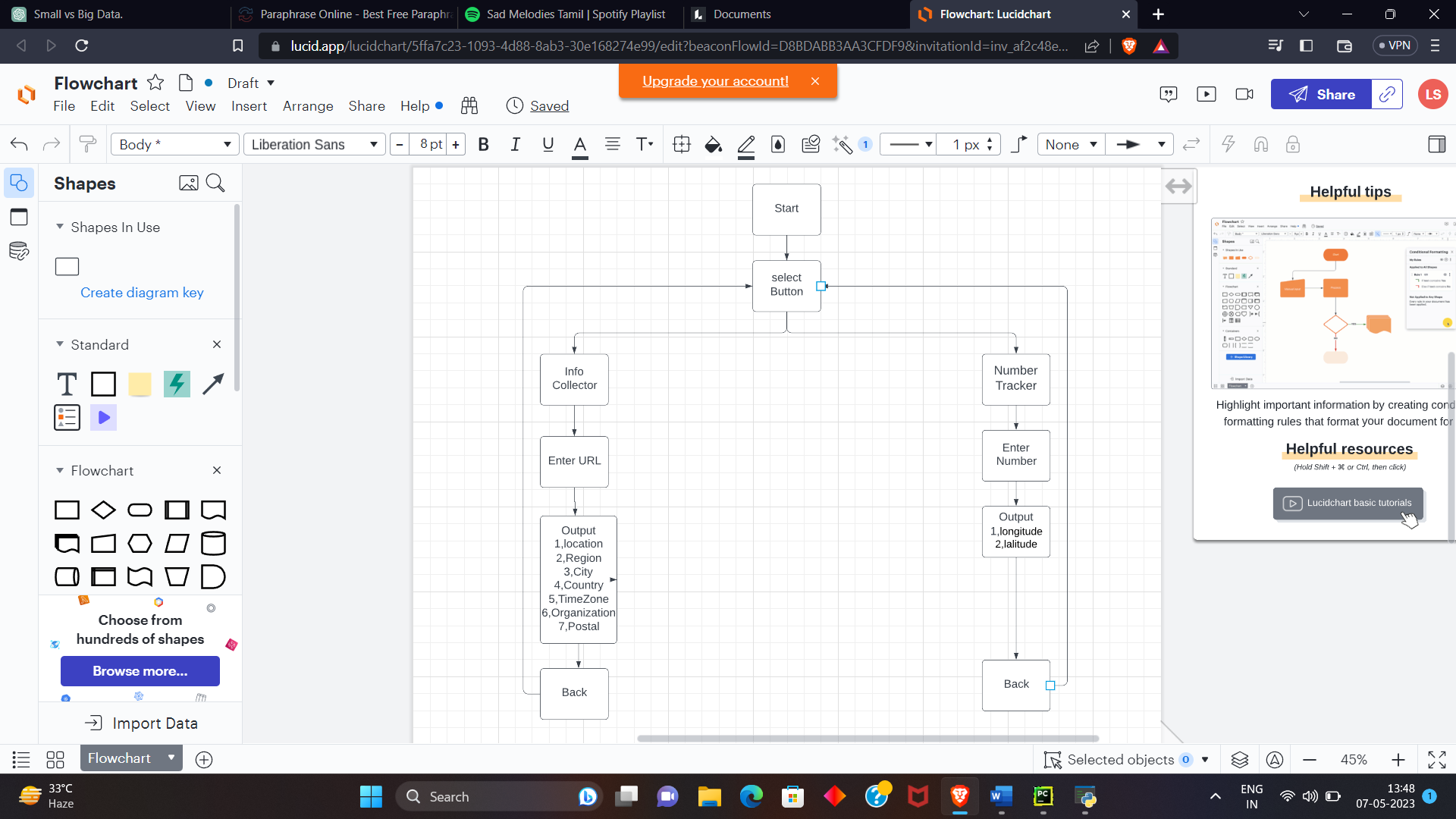
**CHAPTER 5**

# SYSTEM DESIGN

## 5.1 DATA FLOW DIAGRAM:

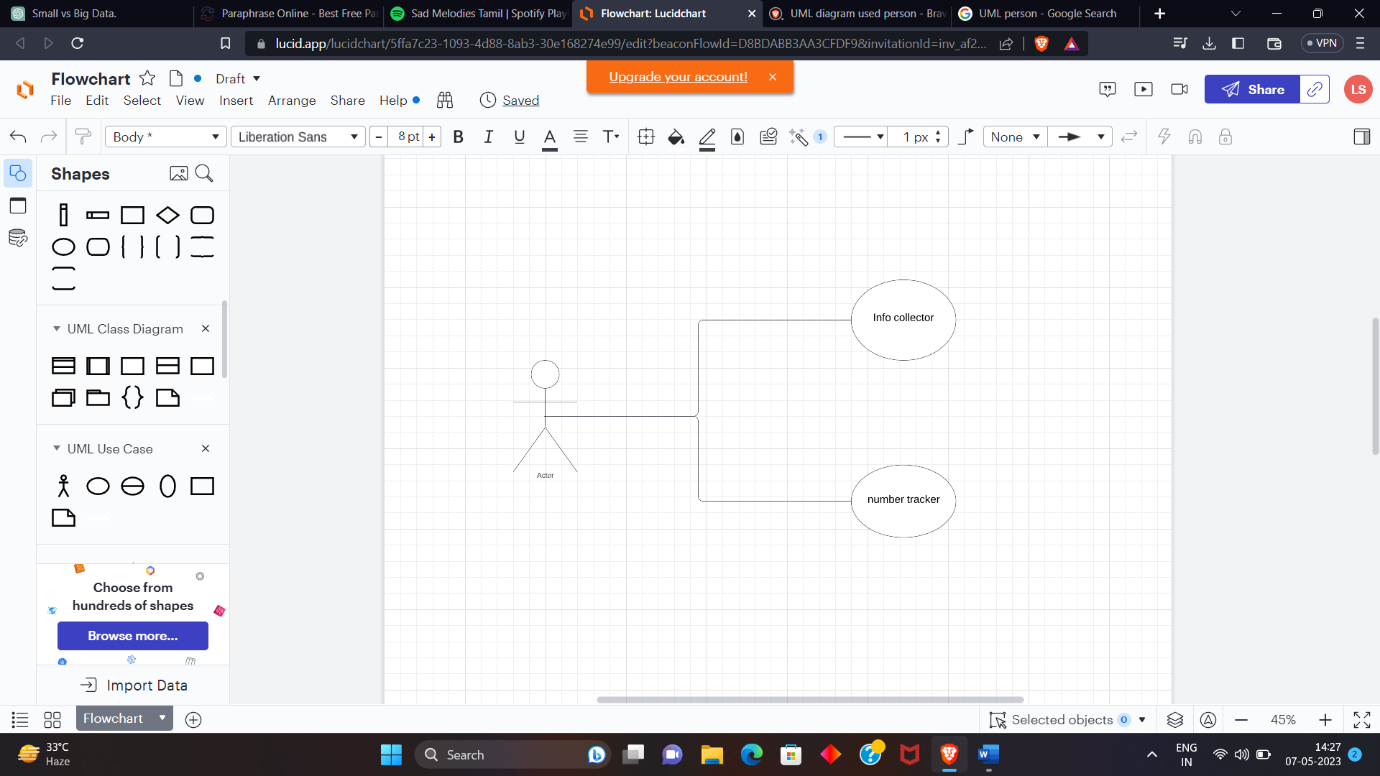


**5.2 ER DIAGRAM:**

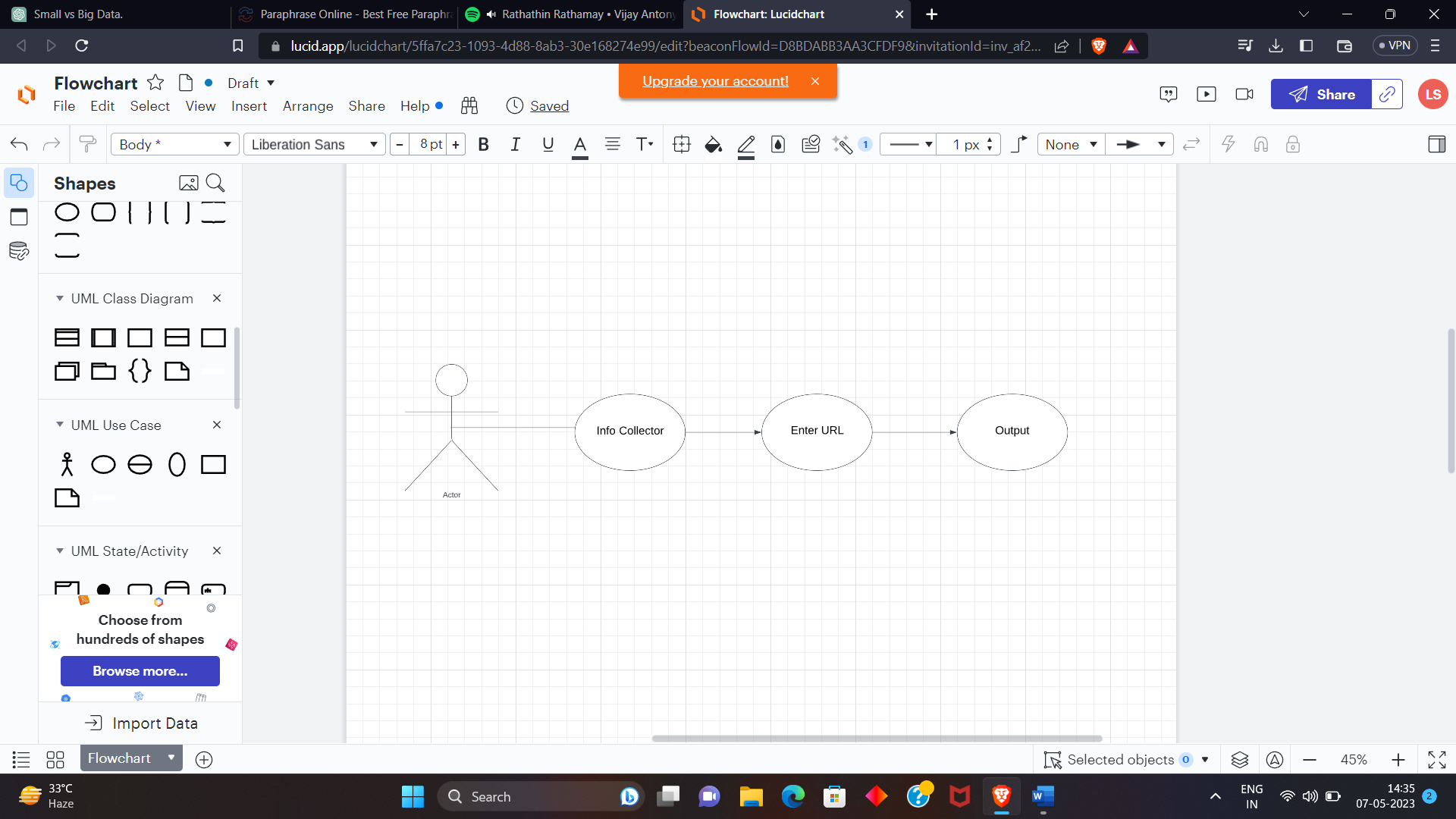


**5.3 USECASE DIAGRAMS:**

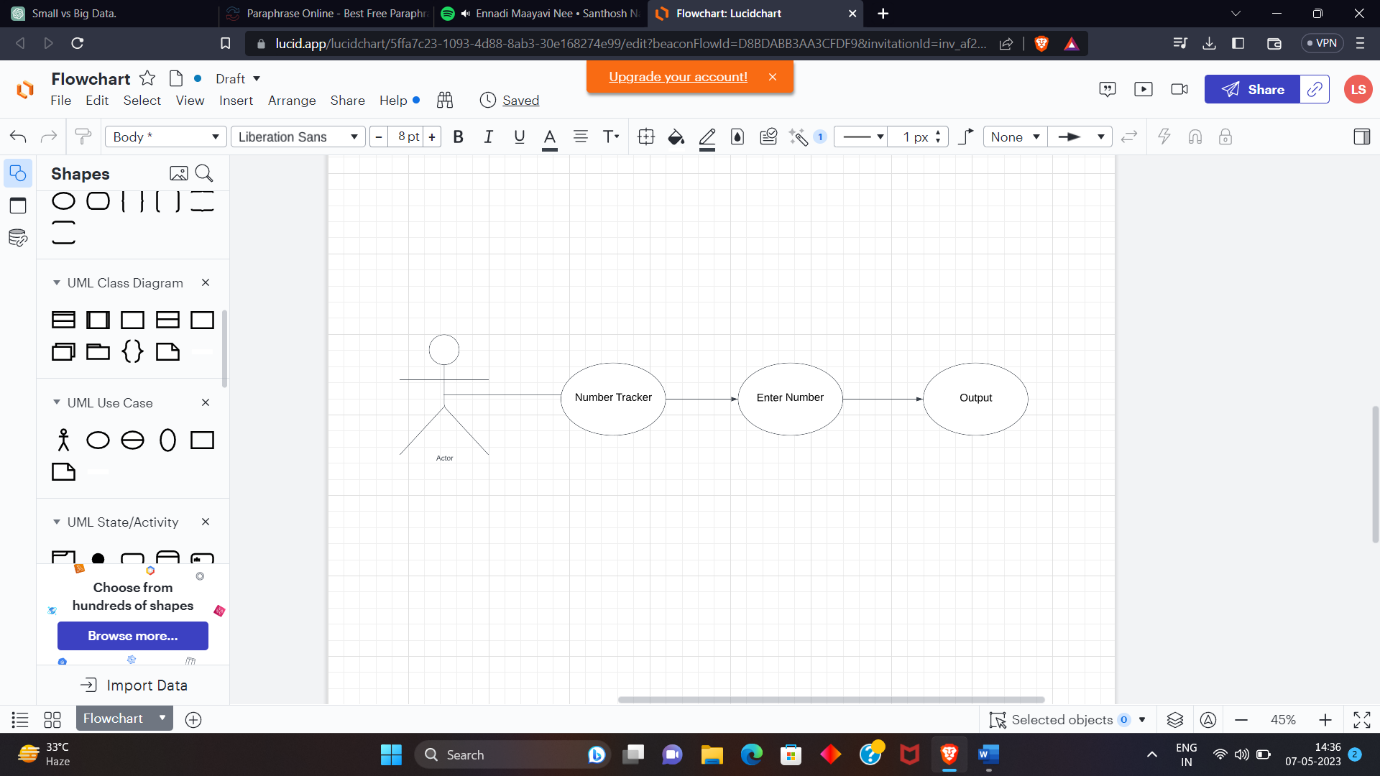
**Usecase diagram for selecting tools:**

****

**Usecase diagram for Info Collector:**



Usecase diagram for number tracker:



**CHAPTER 6**

# SYSTEM IMPLEMENTATION

6.1 Selecting Button:

Clicking button can help organizations collect relevant information and track key metrics that can be used to optimize their operations, improve customer experience, or drive business growth. However, it is important to ensure that data collection and tracking practices comply with applicable laws and regulations, as well as user privacy and security requirements.

Clicking two buttons such as Info Collector and Number Tracker may refer to a process or action taken in various contexts such as in software applicationTop of Form

6.2 Info Collector:

We can gather information about a website by using the info collector button. First, we go to the info collector page and enter the website's URL, like "www.google.com". Then we press search, and the program gives us information about the website, like its IP address, location, region, city, country, timezone, organization, and postal code. This can help us learn more about the website.

6.2 Number Tracker:

The number tracker button helps us find the location of a phone number. It shows the latitude and longitude of the location, as well as the company it belongs to. To use it, enter the victim's phone number in the format of +91 \*\*\*\*\*\*\*\*\*\*\*. The program will then display the information. This module will be improved in the future to make it even better.

**CHAPTER 7**

# CONCLUSIONS AND FUTURE WORK

In conclusion, information gathering through the use of URL and phone number can be valuable for various purposes, including marketing research, lead generation, customer profiling, and more. The URL can provide valuable information about a website, including its content, structure, and metadata, while the phone number can be used to collect contact information and gain insights into a person's behavior and preferences. However, it is important to ensure that such practices comply with applicable laws and regulations, as well as ethical and privacy considerations. Organizations should take measures to protect user data and use it only for legitimate purposes while being transparent about their data collection and processing practices. By doing so, they can build trust with their customers and stakeholders and leverage the power of information to drive business growth and innovation.

Using tools like penetration testing, web analysis, and system analysis to collect information and track numbers is a better way to collect and analyze data. These programs are made in a coding language called Python and are meant to be used for learning. They help you find weaknesses in computer systems, understand what data is being sent over the internet, and keep track of important measures and results.

These tools are easy to use and understand, so even people who are new to programming can use them. This means more people can get help from these tools. To improve how businesses work, we can make computer programs that are faster and better at collecting and analyzing information. This will help organizations make smarter choices and get things done more efficiently.

It's important to use these tools in the right way- being fair, following laws, and being open about what you're doing. Companies need to follow the rules and laws that apply to them and make sure they protect users' privacy and safety. We can use technology to make progress in a good way by being careful and fair when collecting and analyzing

information.

CHAPTER 8

Source Code:

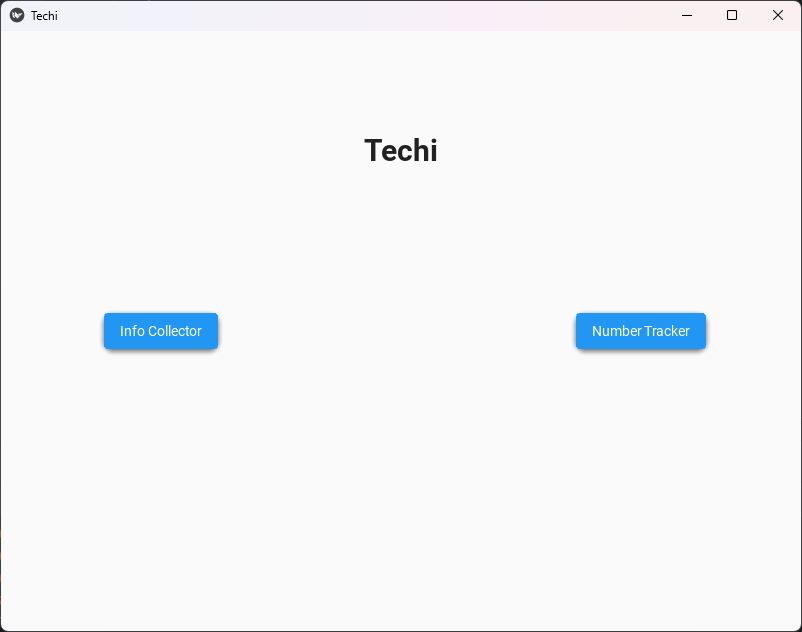
Info Collector:

import socket  
import json  
import requests  
  
def run():  
 url = input("ENTER THE URL TO SCAN >> ")  
  
 print("THE IP FOR " + url + " IS ", socket.gethostbyname(url))  
  
 host\_ip = socket.gethostbyname(url)  
  
 req\_two = requests.get("https://ipinfo.io/" + host\_ip + "/json")  
 resp\_ = json.loads(req\_two.text)  
  
 print("Location: " + resp\_["loc"])  
 print("Region: " + resp\_["region"])  
 print("City: " + resp\_["city"])  
 print("Country: " + resp\_["country"])  
 print("Timezone:" + resp\_["timezone"])  
 print("Org:" + resp\_["org"])  
 print("Postal:" + resp\_["postal"])

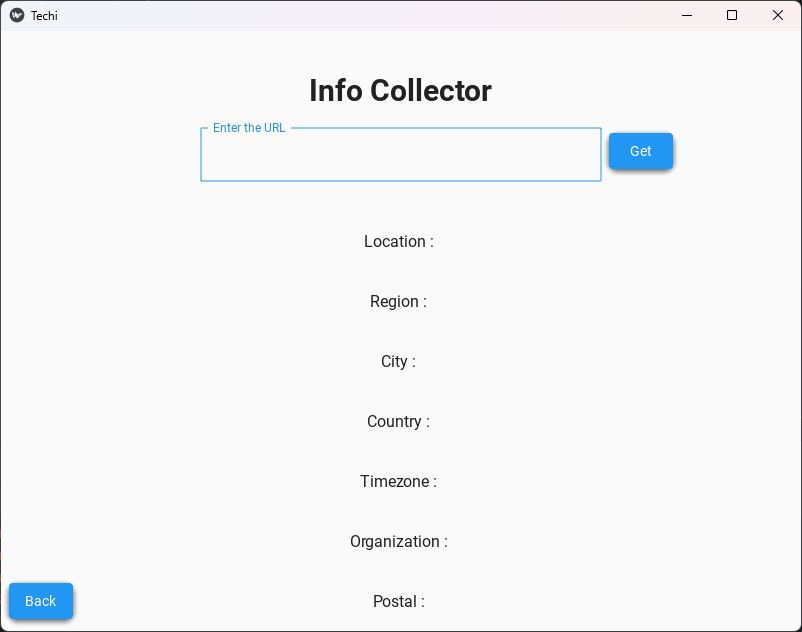
Number Tracker:

import phonenumbers  
import opencage  
import folium  
from phonenumbers import geocoder  
  
print("ENTER +91 ...")  
number = input("enter ur number: ")  
  
pepnumber = phonenumbers.parse(number)  
location = geocoder.description\_for\_number(pepnumber, "en")  
print(location)  
  
from phonenumbers import carrier  
  
service\_pro = phonenumbers.parse(number)  
print(carrier.name\_for\_number(service\_pro, "en"))  
  
from opencage.geocoder import OpenCageGeocode  
  
key = '4edf23a515ba4f1e910f3b1824748aaf'  
  
geocoder = OpenCageGeocode(key)  
query = str(location)  
results = geocoder.geocode(query)  
  
  
lat = results[0]['geometry']['lat']  
lng = results[0]['geometry']['lng']  
  
print(lat, lng)  
  
mymap = folium.Map(location=[lat, lng], zoom\_start=9)  
  
folium.Marker([lat, lng], popup=location).add\_to(mymap)  
  
mymap.save("mylocation.html")

SNAPSHOT:

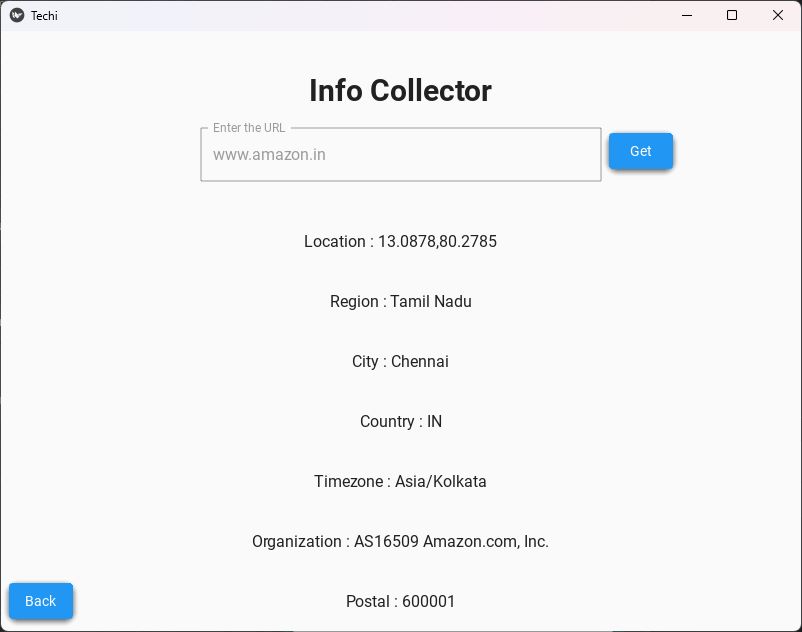


Info Collector:

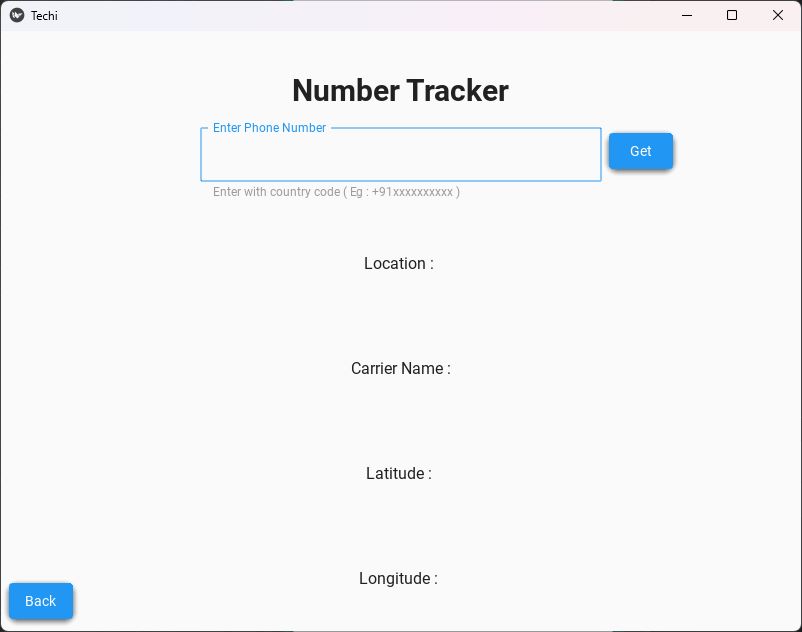


Info Collector :

(OUTPUT)

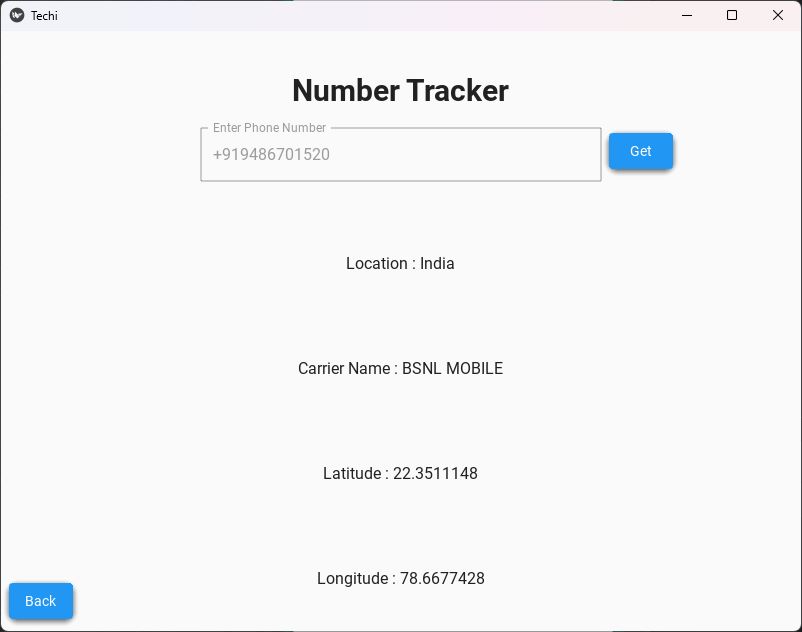


Number Tracker:



Number Tracker:

(OUTPUT)



**CHAPTER 10**

**REFERENCES**

1. <https://null-byte.wonderhowto.com/how-to/find-identifying-information-from-phone-number-using-osint-tools-0195472/>
2. <https://pentesttools.net/how-to-find-information-from-a-phone-number-using-phoneinfoga/>
3. <https://hakin9.org/phoneinfoga-advanced-information-gathering-osint-framework-for-phone-numbers/>
4. <https://github.com/jaisinghaniamit121/InfomationGathering>
5. <https://github.com/weiyangye/Info_Gathering>
6. <https://docs.python.org/3/library/trace.html>
7. <https://github.com/shubhamg0sai/phone-number-tracker>
8. <https://github.com/thornomad/django-hitcount>
9. <https://github.com/4mritGiri/NumberTracker/blob/main/PhoneNumberDetails.py>