KEIZAI TECH.

PROJECT NAME:	IP Logger
DEVELOPER:	Samuel Bueno Francisco

1. STRATEGY & PRODUCT FOUNDATIONS

1.1. SCOPE

The project aims to enable users to input a standard URL into our tool, which will then generate a shortened or masked link suitable for sharing with any individual. Clicking this shortened link records the user's IP address and location in a MySQL database. This data then feeds into a Google Maps API, which displays the precise location of the individual or machine that interacted with the masked link.

Initially, the project aimed to replicate all functionalities of the official IP Logger tool (https://www.iplogger.com/). However, due to difficulties in building every part of the suite from scratch—including challenges with authentication, MVC design patterns, and the Google Cloud API—the project's scope was narrowed. It now focuses exclusively on refining the URL shortener and masker.

We plan to prioritize the development and shipment of the IP Logger tool before continuing work on the main IP Tools Suite. The latter will be addressed at a later stage.

1.2. VISION AND POSITIONING

The vision and positioning of the project regards the tool being a robust, user-friendly solution for tracking IP addresses and locations through masked URLs. We aim to position it as a critical asset for security professionals, digital marketers, and anyone needing to verify the geographical origin of interactions with shared links. Our tool will stand out by offering precise location data visualized on Google Maps, combined with an intuitive interface for generating and managing masked URLs.

1.2.1. PROBLEM STATEMENT

Considering Brazil's historical and ongoing security deficiencies, coupled with the nation's precarious position on the verge of becoming a narco-state, it is imperative to develop and implement tools designed to protect against and combat the influence of drug traffickers, fraudsters, corrupt officials, and other malicious entities.

This project focuses on developing a tool that empowers customers to combat malicious actors. It utilizes a "reverse phishing" technique where the scammer is "trapped" into revealing their location and data. This is achieved through a precisely designed computer algorithm made to be run on the web, which means users do not need to install additional software or modules onto their personal devices.

1.2.2. TARGET USERS

The primary target users for the IP Logger tool are:

- **Security Professionals:** Individuals or teams who require precise IP and location data for threat intelligence, incident response, and cybersecurity investigations.
- **Law Enforcement and Investigators:** Agencies and individuals involved in combating cybercrime, fraud, and other illicit activities, who can leverage location data for investigative purposes.
- **Journalists and Researchers:** Individuals who need to verify the origin of digital interactions or protect sources by understanding who is accessing shared information.
- **General Users Concerned with Online Security:** Anyone who wishes to protect themselves from online scams, verify the authenticity of links, or understand the geographical origin of interactions with their shared content.

1.3. BUSINESS REQUIREMENTS

BR01: Google API keys must be securely stored within the project folder structure to prevent unintentional leaks.

BR02: The app must abide by privacy laws of the following countries:

Andorra, Australia, Austria, Belgium, Brazil, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Ireland, Israel, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Taiwan, United Kingdom, and the United States.

BR03: Users must have the ability to request the removal of their associated data by developers or the system at any time.

BR04: Users need the ability to select whether their shortened or masked link will expire.

BR05: Each link generated by the user has an inherently defined and concealed "expiry date," regardless of their decision to not set an expiration for their links. This measure is implemented to safeguard user information, as malicious actors may attempt to exploit the tool for nefarious purposes.

BR06: The implementation of the MVC design pattern is not required for this project.

BR07: Each generated link ought to produce a password known solely to the individual who initiated its creation, thereby ensuring that only the link's originator can access click data and target information.

1.4. FUNCTIONAL REQUIREMENTS

FR01: The app is built to be publicly available, therefore, there is no need to implement a login mechanism.

FR02: The user must be provided a checkbox that says "my link does not expire", should they choose not to expire their link.

FR03: The generated links must be listed in a table with the following information/columns:

a. The unique identifier for the link/number, which is utilized to monitor the volume of links generated and to assign a distinct value to each.
b. The shortened link;
c. The original link;
d. The date of creation;
e. The date of expiry (if it does not exist, the column should read "does not expire"

FR04: The target’s information must be presented in a table with the following columns:

a. A unique identifier;
b. Short Code;
c. IP Address;
d. Accuracy;

e. Precise Address;
f. City;
g. Country
h. Device type (desktop computer/mobile)

1.5. STACK USED

FRONTEND TECHNOLOGIES:

- HTML5
- CSS3
- JavaScript
- jQuery (with AJAX)
- Bootstrap CSS
- FontAwesome CDN (for icons)
- Google Fonts CDN (for fonts)
- Google Cloud Maps API

BACKEND SPECIFICATIONS:

- **PHP:** Version 8.4
- **MySQL RDBMS:** Version 5.7.44
    - **Hostname:** localhost (UNIX socket: /var/lib/mysql/mysql.sock)
- **Web Control Panel:** DirectAdmin dashboard

SYSTEM OVERVIEW

- Hostname: server39.srvlinux.info
- Control Panel: DirectAdmin
- Technology Stack: PHP 8.4 and MySQL 5.7.44 (connected via local UNIX socket)

OPERATING SYSTEM AND KERNEL

- Kernel Version: 3.10.0-962.3.2.lve1.5.85.el7.x86_64

- Distribution: CloudLinux LVE, EL7 generation

CPU

- Model: Intel Xeon E3-1240 v6 @ 3.70 GHz
- Cores/Threads: 4 cores / 8 threads
- Capabilities: AVX2, AES-NI, VT-x

MEMORY

- Installed RAM: Approximately 16 GB (CommitLimit ≈ 15.5 GB)

- Swap: 0 GB (no swap configured)

STORAGE AND FILESYSTEMS

Root (/): /dev/md126, 226 GB total space, about 49% used

/tmp: /dev/sdc, 1.8 TB total, about 68% used

/dev/shm: tmpfs, 16 GB

CONFIGURATION NOTES

No system swap is configured, which increases the risk of running out of memory during peak load.

MySQL 5.7 is a legacy version; consider planning an upgrade to MySQL 8.0 LTS.