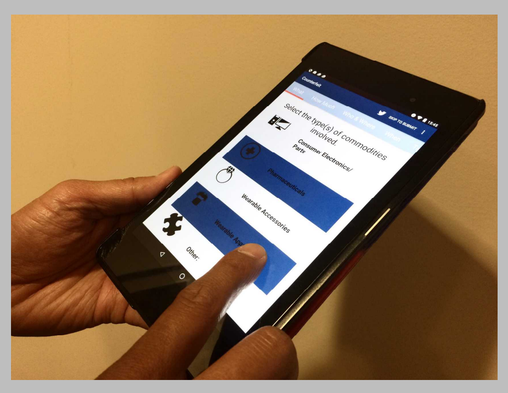
SAND2016-6968D

Exceptional service in the national interest

Sandia National Laboratories



Homeland Security

Science and Technology

Reporting Fraud Using Mobile Apps

Interns

Kyle Burns | San Ramon Valley High School
Sarina Kapai | USC | Electrical Engineering
Vinod Krishnamurthy | UCSC | Computer Science
Tanner Summers | Cal Poly Pomona | Computer Science

Project Managers

Matthew Wong | 08954 | Quantitative Modeling & Analysis
Andrew Cox | 08116 | Systems Research & Analysis III

Overview

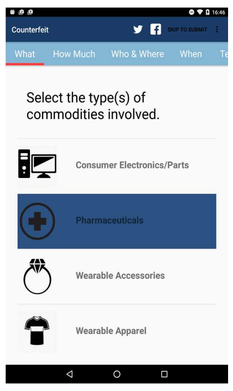
The Counterfeit Mobile Application is a user friendly mobile version of the existing Department of Homeland Security Immigration and Customs Enforcement (ICE) PDF form used to report the selling of counterfeit items. The goal of this investigation is to make it easier for the general public (specifically consumers between the ages of 18 and 30) to report fraudulent sales related to intellectual property (IP) violations. The project ultimately intends to utilize Citrus, a web-crawling and text analytics software framework to assemble the massive amounts of data expected to be collected from this app, using machine learning to ignore irrelevant reports. The software will assist in identifying patterns in the fraudulent activity reported by user, which can be used to track and perhaps anticipate other counterfeit products in the area. A bar code scanner may be added to check UPC codes for validity. Users can also submit photos of the items. With the rise in use of mobile devices, the mobile application can help decrease fraudulent sales of dangerous counterfeit items such as pharmaceuticals, faulty automotive parts, electronics, skin creams, and possibly even foods. It is important to stop the sales of counterfeit items, not only for the companies that sell the legitimate products, but for the safety of the general public.

User Experience

Starting Page

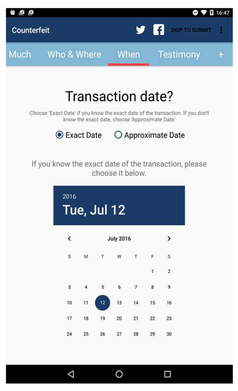
We wanted the design of this app to be user-friendly. This will increase the ease and speed of reporting sales of counterfeit items, helping to yield higher quality and quantity of IP violation reports to ICE. The user is presented with a splash screen that shows the DHS seal, remaining there until the app has fully loaded. The user is then given the option to report anonymously or not. Both options take the user to a tabbed style layout in which the tabs at the top of the screen indicate a clickable or swipe-able way to transition between pages. To move to the next page, all the user has to do is swipe to or click on the next tab using the tab bar at the top of the application. This design will allow us to reach a wider audience, because the mere idea of filling out a length PDF form could discourage completion. A mobile application would encourage more people to submit the valuable information. Each tab has unique features to draw the attraction of the user. The initial beta app will be deployed on Android devices.

The screen to select the type of counterfeit item uses a dynamically growing list that allows multiple clicks and looks appealing to the user. The list allows the user to select which items they want to report at a very fast rate, through simply tapping on the commodity of interest.



Fraudulent Item Selection Page

Another feature of the app is a calendar component for the page that records when the transaction occurred. The original form simply asked when the transaction occurred, but to make the app more user friendly and appealing, we implemented a selectable calendar in which the user could click on the date of the transaction rather than typing it in.

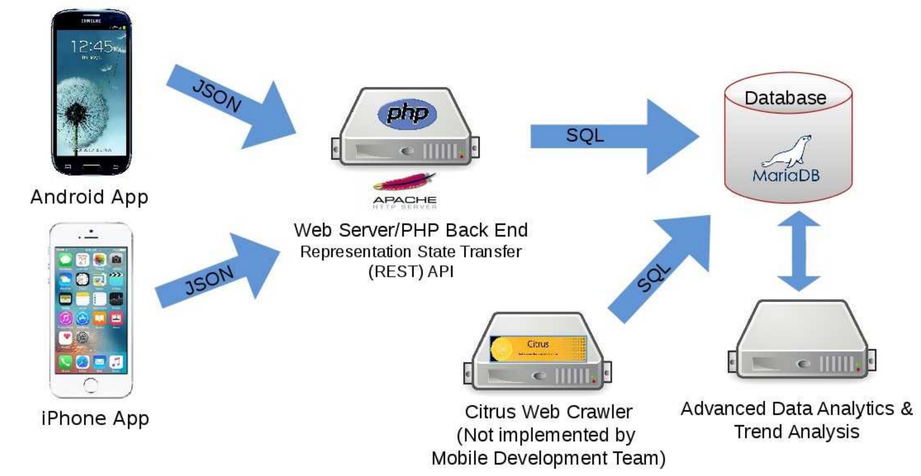


Date of Transaction Page

iOS Version

With 43% of all smartphones in the U.S. being Apple devices, an iOS version of the app is also necessary. The iOS version is made to share most of the traits that the Android version uses, while also incorporating traditional iOS characteristics to other iOS apps. With a lower navigation bar, familiar to most iPhone users, the app will allow users to navigate by clicking or swiping across tabs. While the Android version is programmed in Java using Android Studio, the iOS version is programmed in the Swift language using Xcode.

Server Side Processing



The mobile app collects the user data and allocates unique Java objects to hold the data. An object is defined as an instance of a class; a class exhibits behaviors and properties that are defined within it. Each class contains the proper field types and methods that utilize the information from the user.

Regardless of how much information has been filled out, the user can submit the data from any screen. Built-in app libraries convert the objects into a JSON (JavaScript Object Notation) representation, which is a very well-known and widely used form of exchanging information/data between endpoints. The JSON is represented as a string that is sent to a PHP page on a server. The PHP page grabs the information and parses the information accordingly, and divides the information into various SQL (Structured Query Language) queries that populate a database with the data to be analyzed later.

The photos may contain GPS information and other meta-data that will be collected and analyzed. The GPS coordinates can aid in the location of the fraudulent sale while any meta-data collected from the photos could be stored in a NoSQL database such as MongoDB (Mongo Database), while the user-typed information is stored in a relational database such as MariaDB (Maria Database).

This project plans to leverage the Citrus framework developed at Sandia National Laboratories (Org 05635), which will complement this project by providing a web crawler and text analytic tools to help develop counterfeit sales trends. Citrus could also help to automatically discover online stores selling counterfeit merchandise through web crawling and text analysis of the web store's HTML/CSS code. Future features that could be added include voice recording submission (to improve the speed of reporting IP violations), bar code scanning, and obtaining metadata (such as GPS coordinates) from user submitted photos.

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
SAND No. 2011-XXXXP