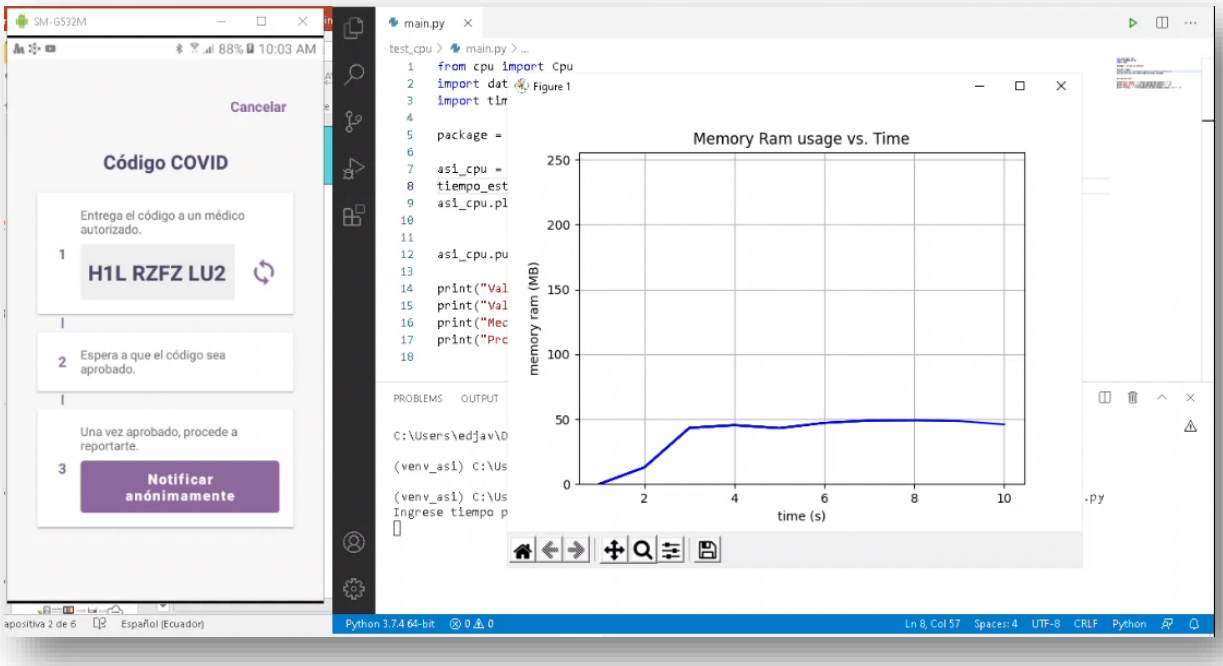
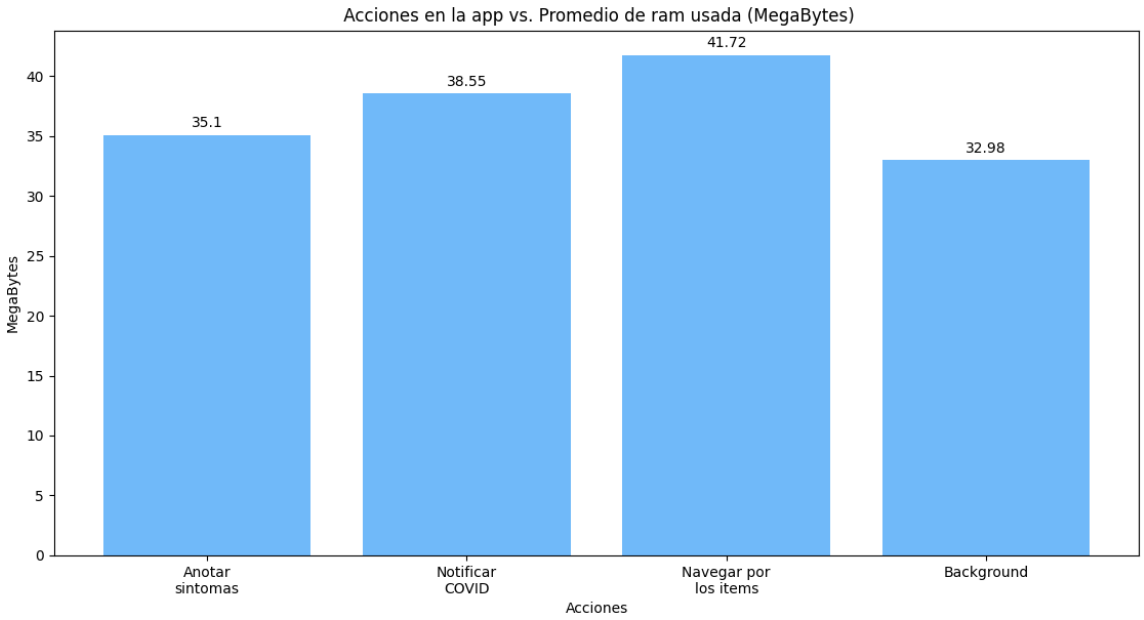
Análisis de caja negra

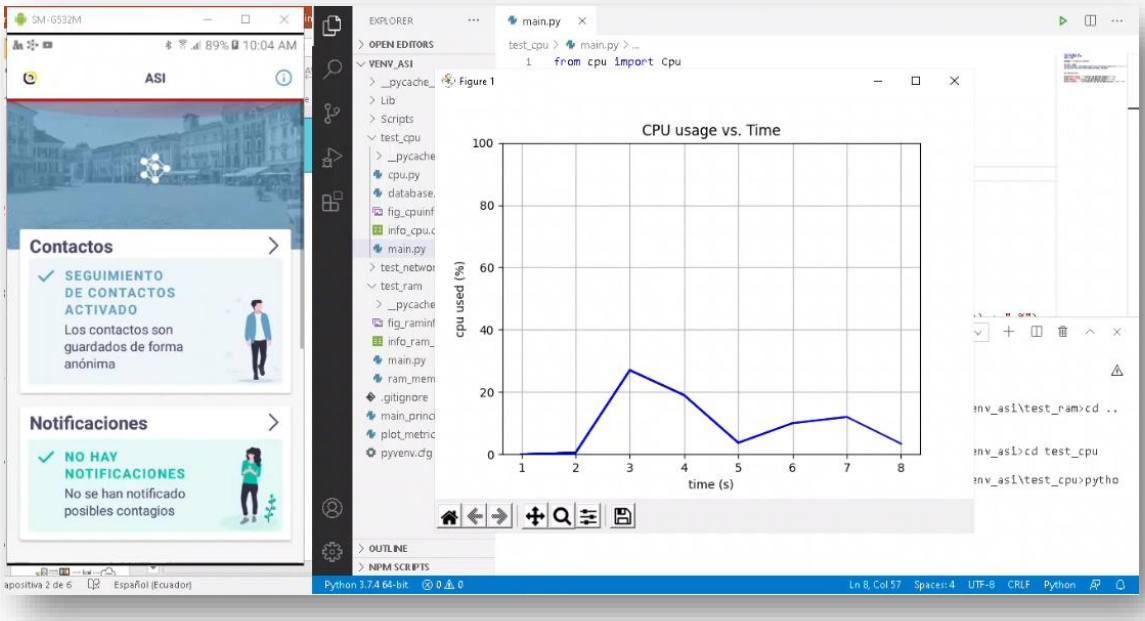
- Test de memoria RAM usado

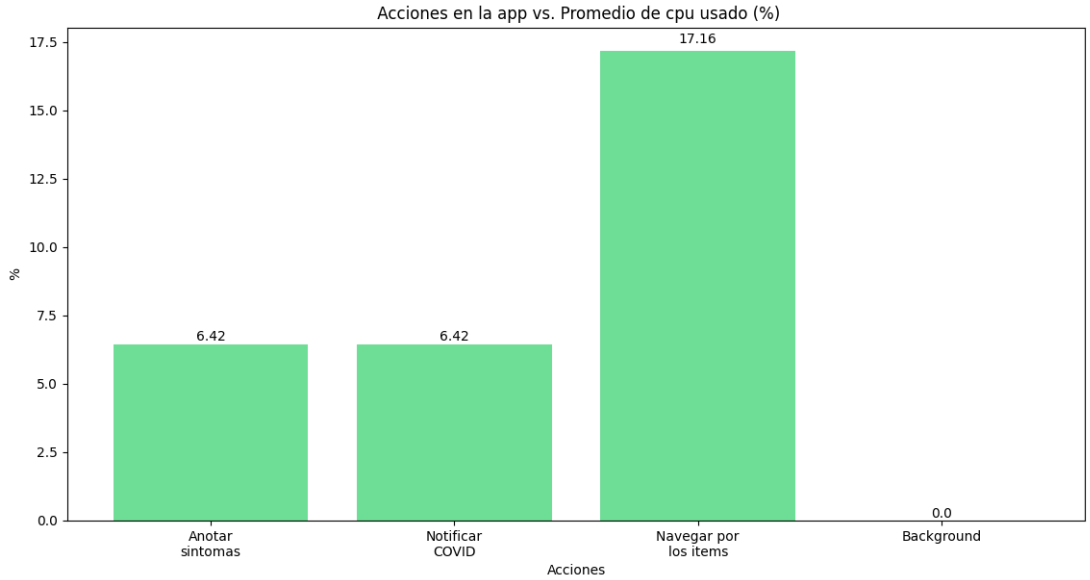




Se realizaron 20 ejecuciones del script en Python por las cuatro acciones que se observan en la figura anterior, logrando cuantificar el promedio de memoria RAM usada por cada acción.

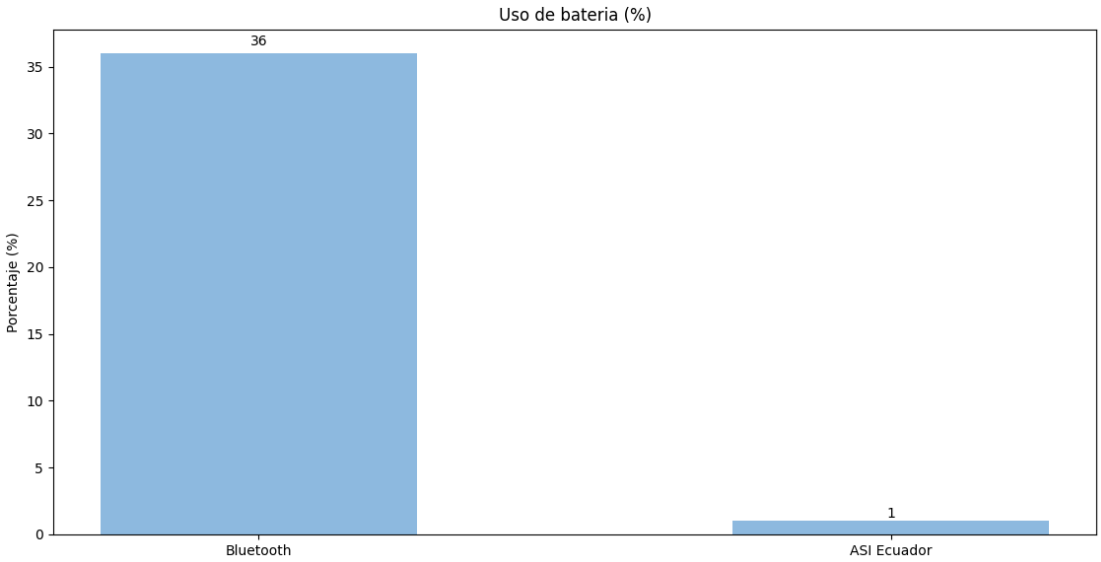
- Test de CPU usado





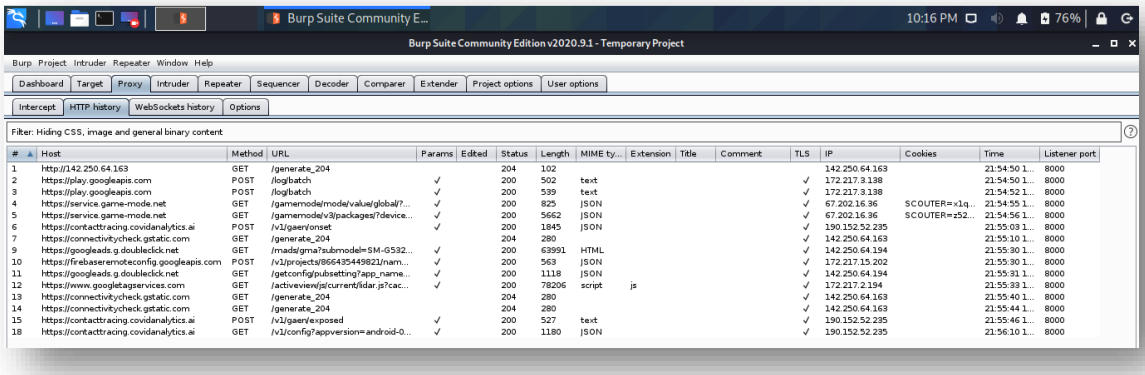
Se realizaron 20 ejecuciones del script en Python por las cuatro acciones que se observan en la figura anterior, logrando cuantificar el promedio de CPU usado por cada acción.

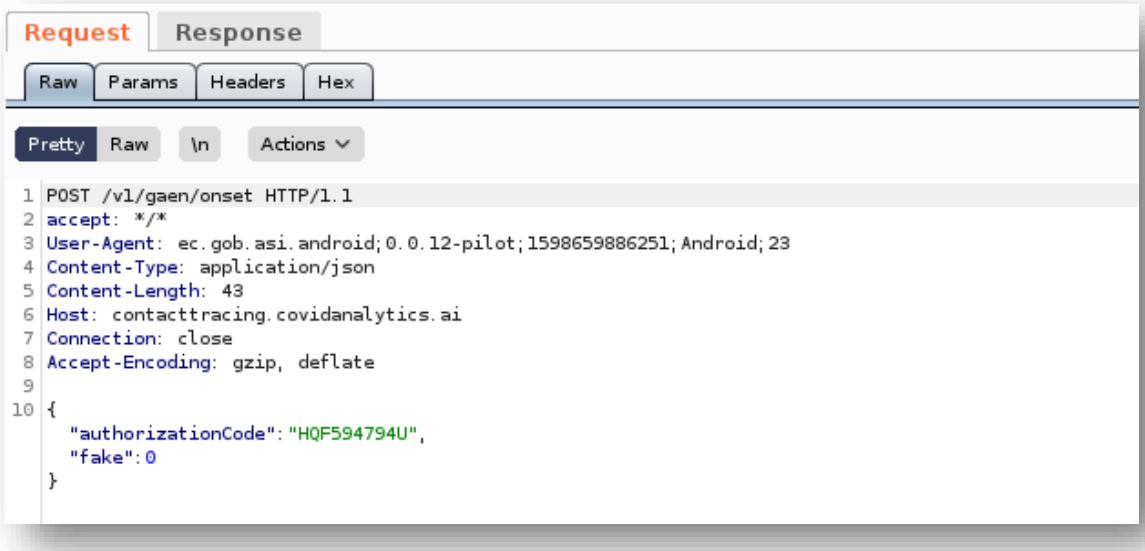
- Recolección del uso de batería

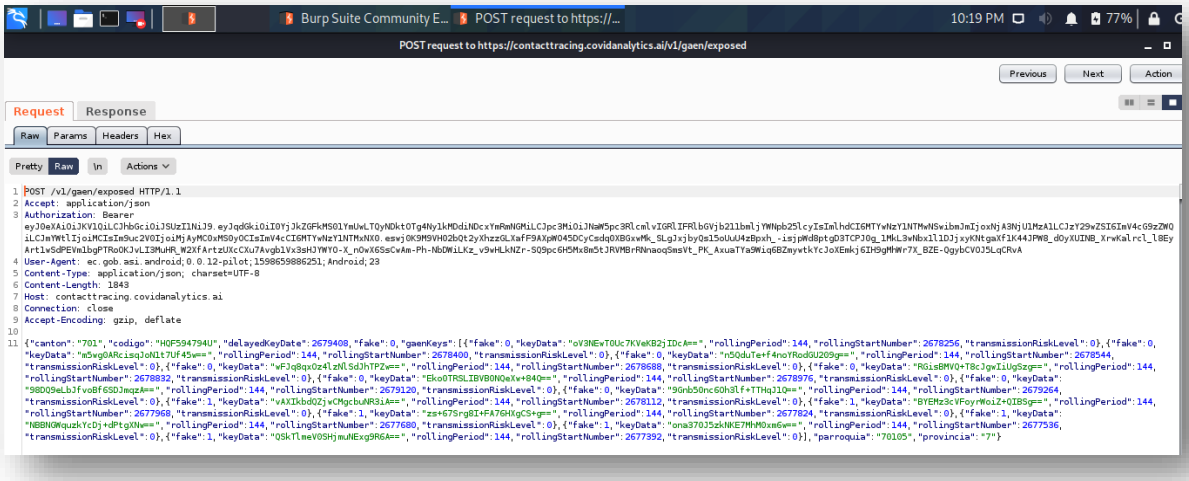


Se recogieron 5 veces los valores de batería usado por la aplicación móvil dejando pasar un día, logando cuantificar el promedio de batería usada.

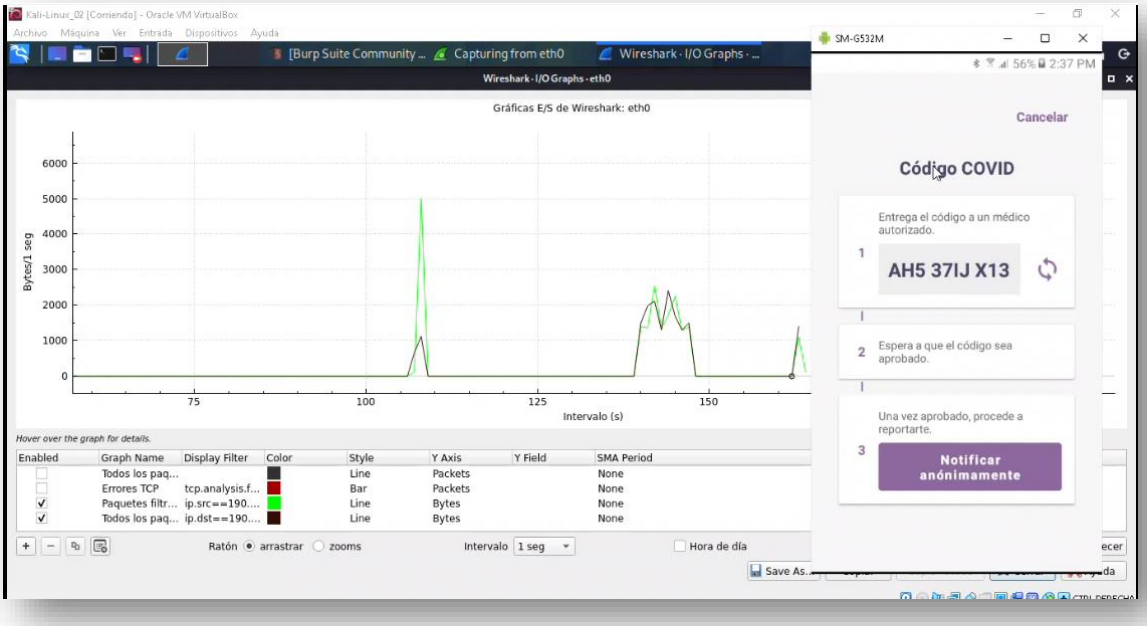
- Test de seguridad básica usando Burp proxy







- Test de red usado por la aplicación móvil

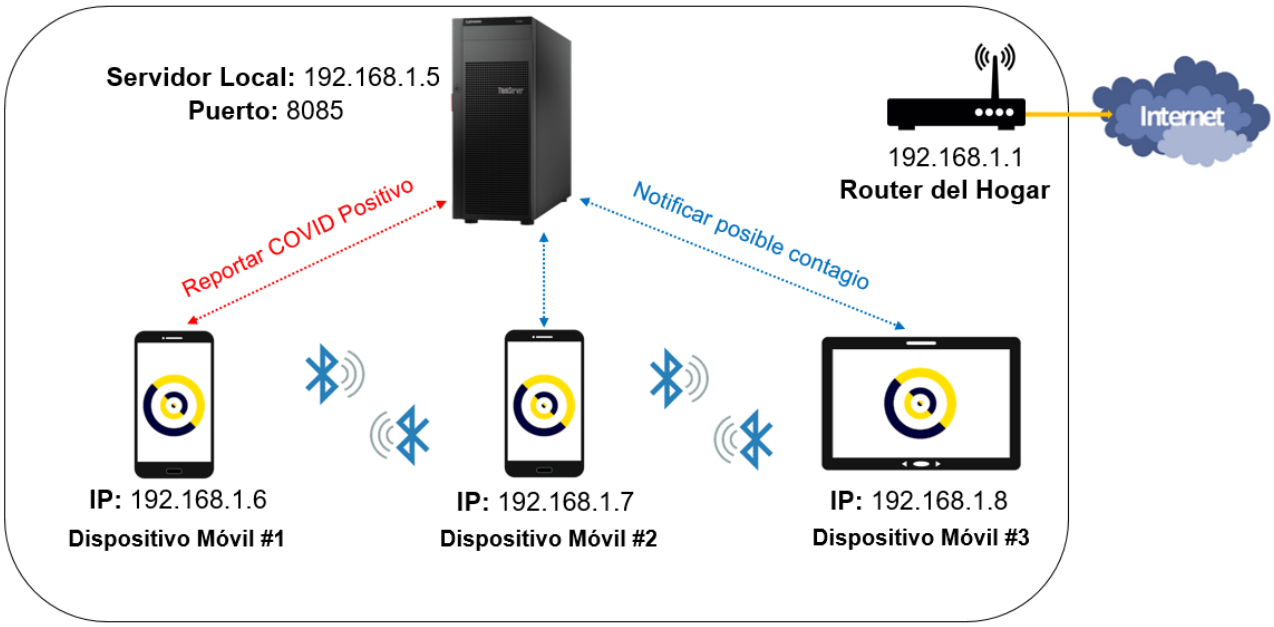


Datos de red de subida y bajada usados por la aplicación móvil al ejecutar por primera vez y cuando se valida el código COVID.

Análisis de caja blanca

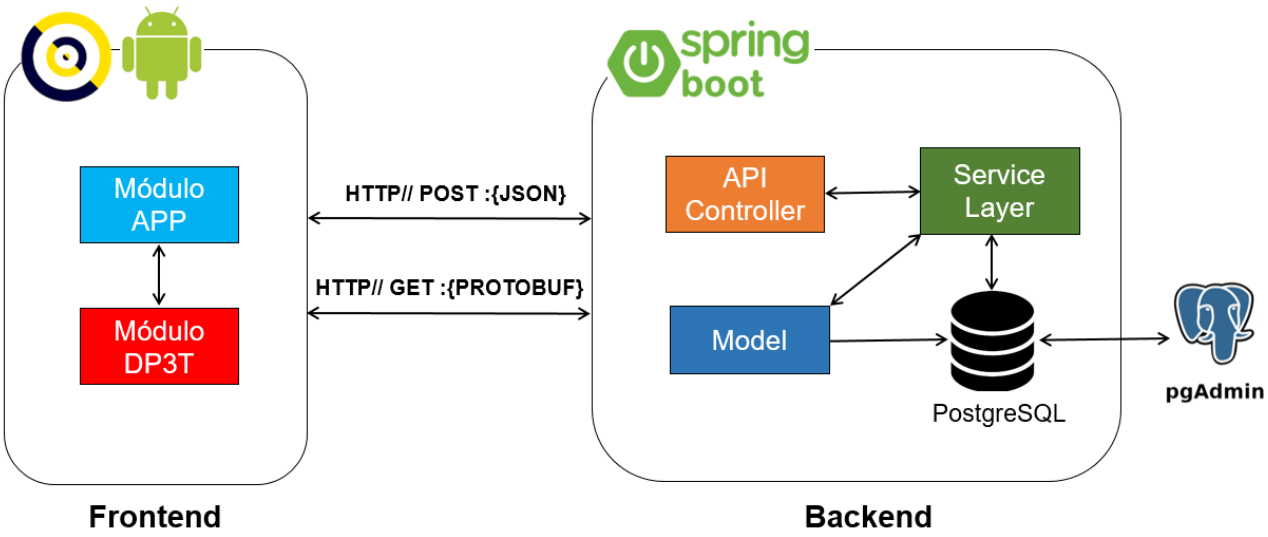
Arquitectura de red

En la imagen se muestran los componentes usados para el entorno simulado. Las pruebas de caja blanca consistieron en estudiar el proceso de intercambio de llaves mediante Bluetooth y la comunicación con el servidor local para reportarnos como COVID positivo y también para notificar de un posible contagio a los contactos.



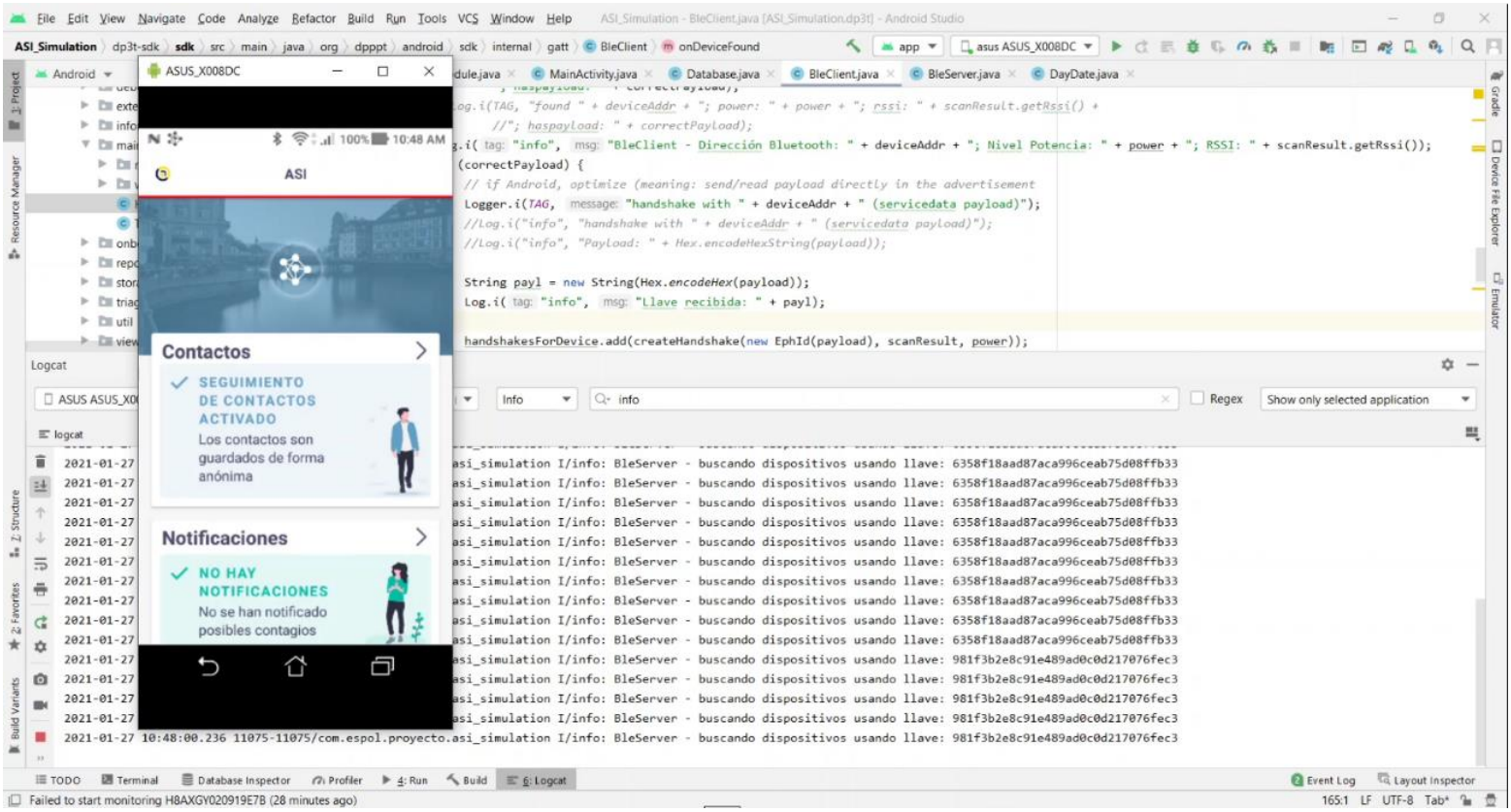
Arquitectura de servicios

El frontend cuenta con dos módulos, APP que tiene el código para la apariencia y DP3T que tiene las funcionalidades para el rastreo de contactos y comunicaciones con la API. El backend está implementado bajo el framework Spring Boot con el patrón MVC y se comunica con su base de datos PostgreSQL, la cual es administrada mediante pgAdmin.

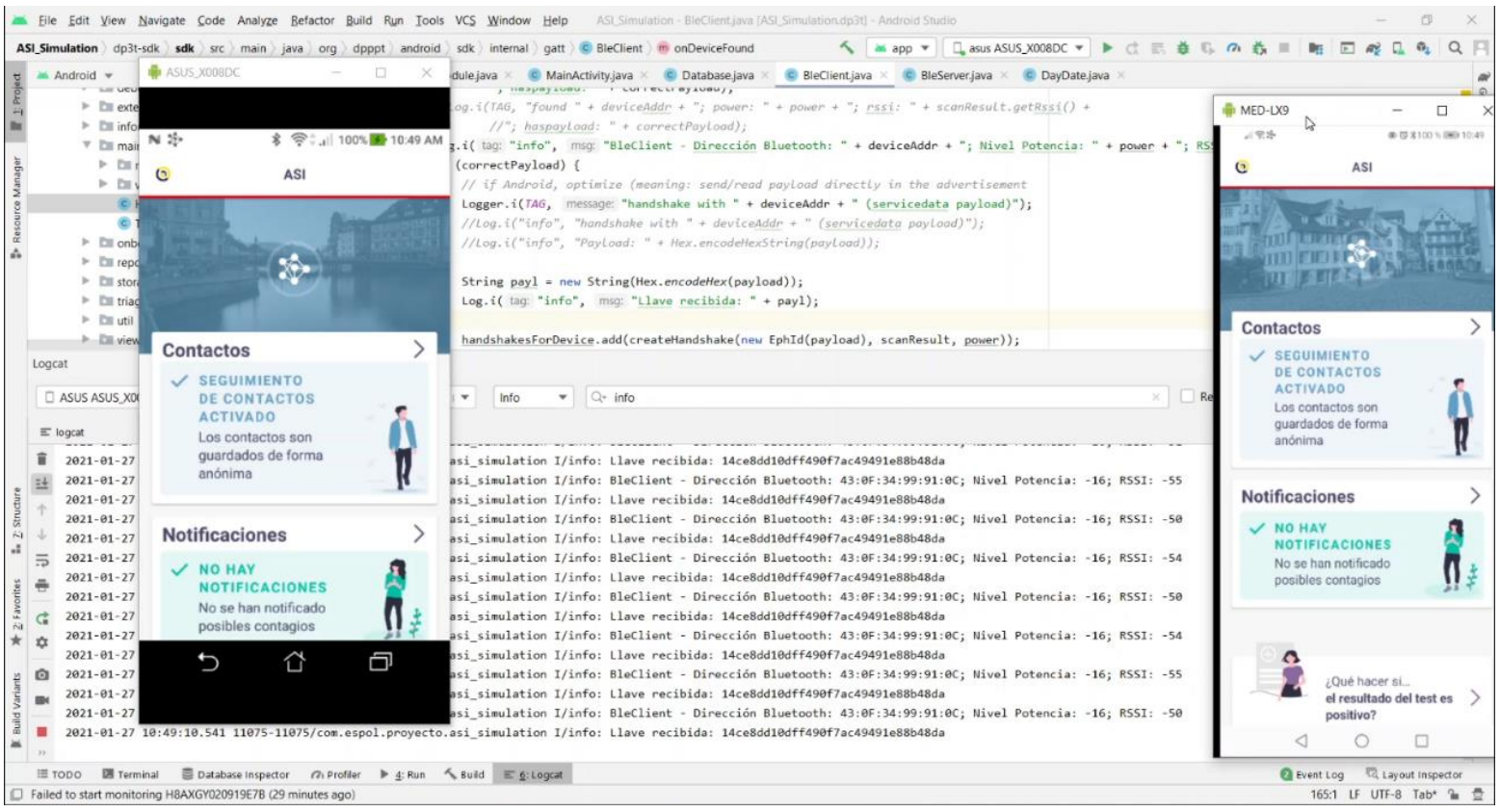


Resultados: Intercambio de llaves mediante Bluetooth

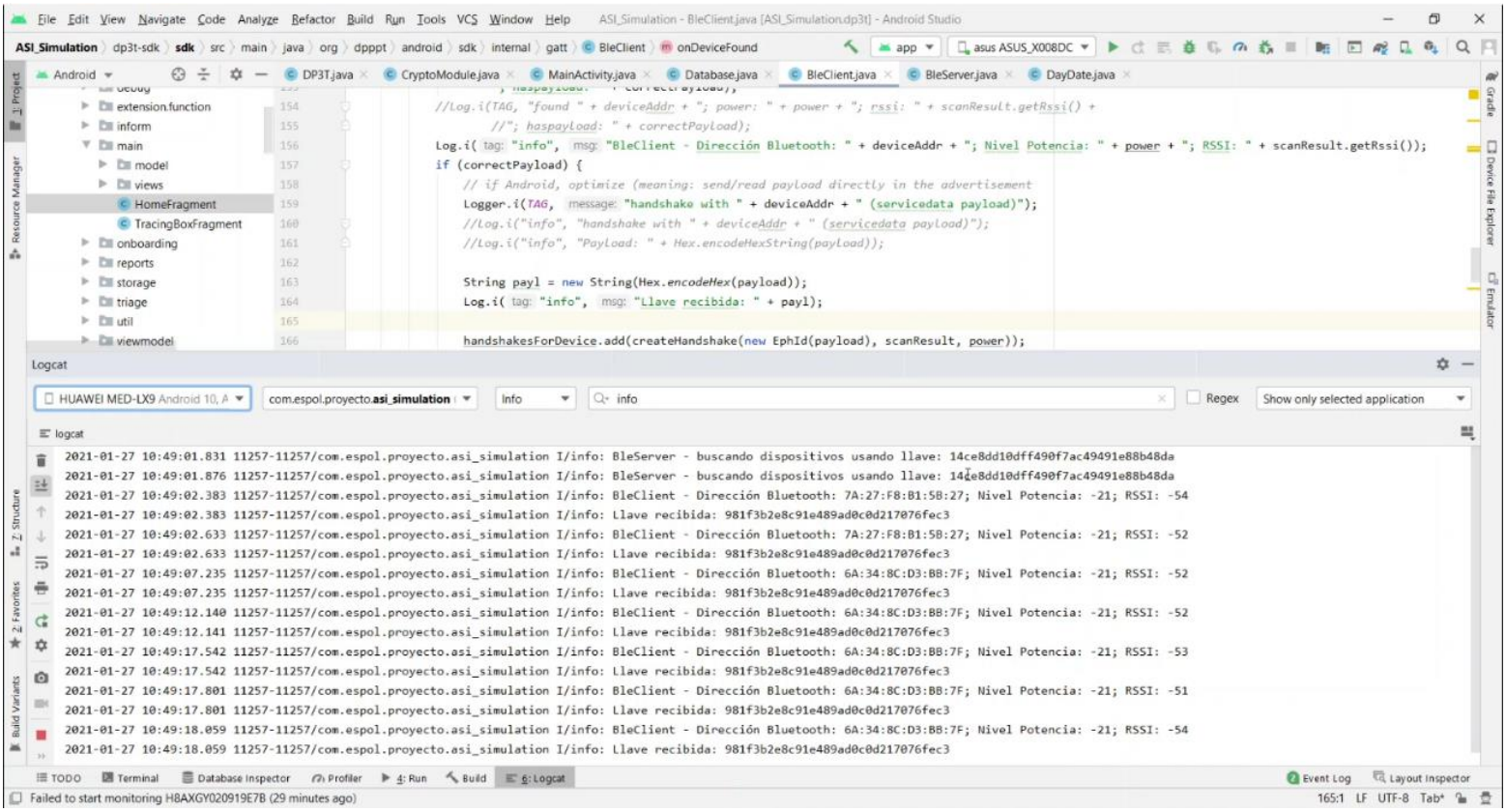
Mediante la herramienta Logcat de Android Studio se imprimen las llaves que utiliza el primer celular para intercambiar con otros dispositivos.



Cuando se coloca otro celular que tiene instalada la aplicación, empieza el intercambio de llaves, como se observa a continuación:

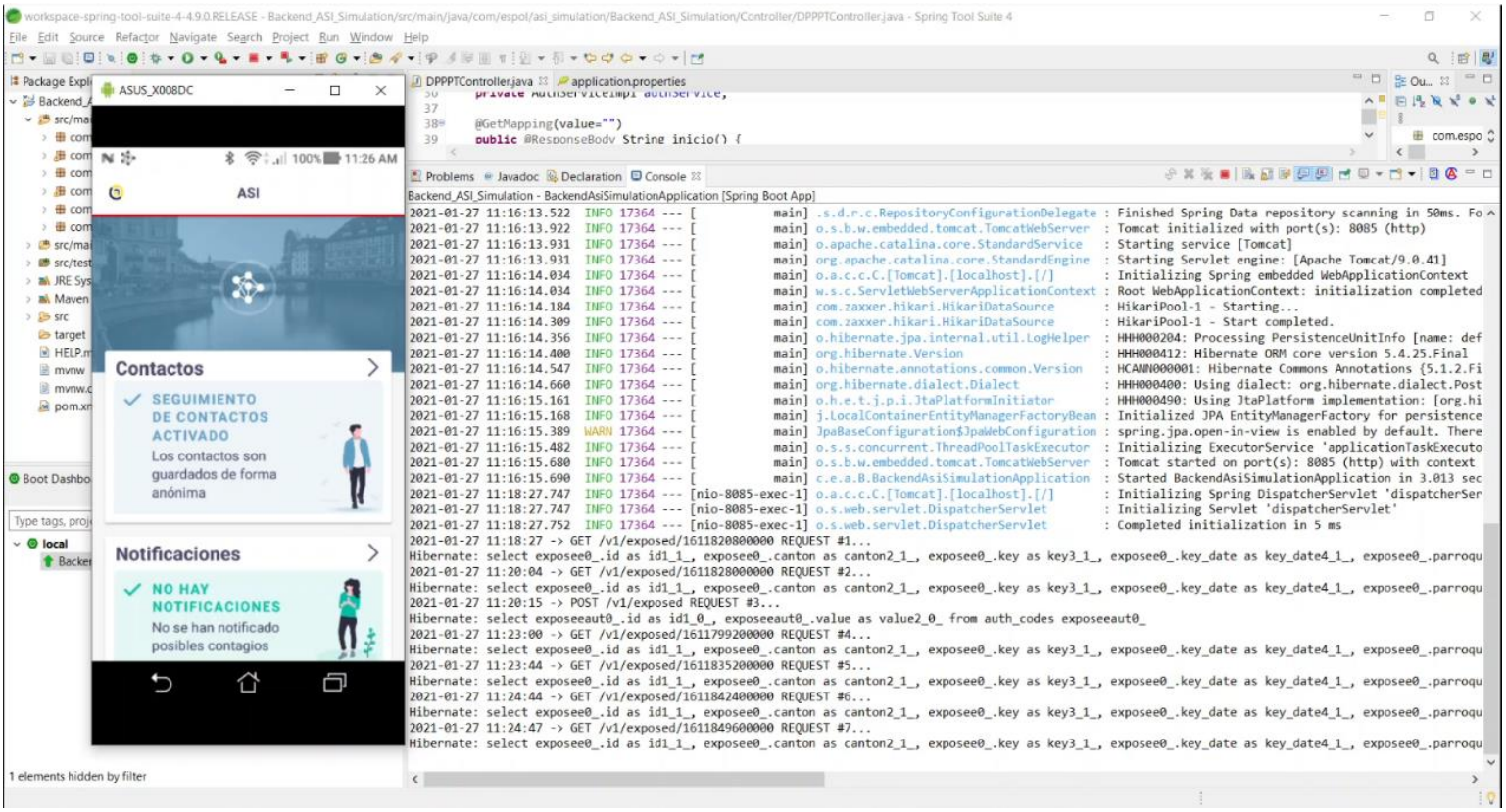


Aquí se muestra, lo que recibió el segundo dispositivo móvil:

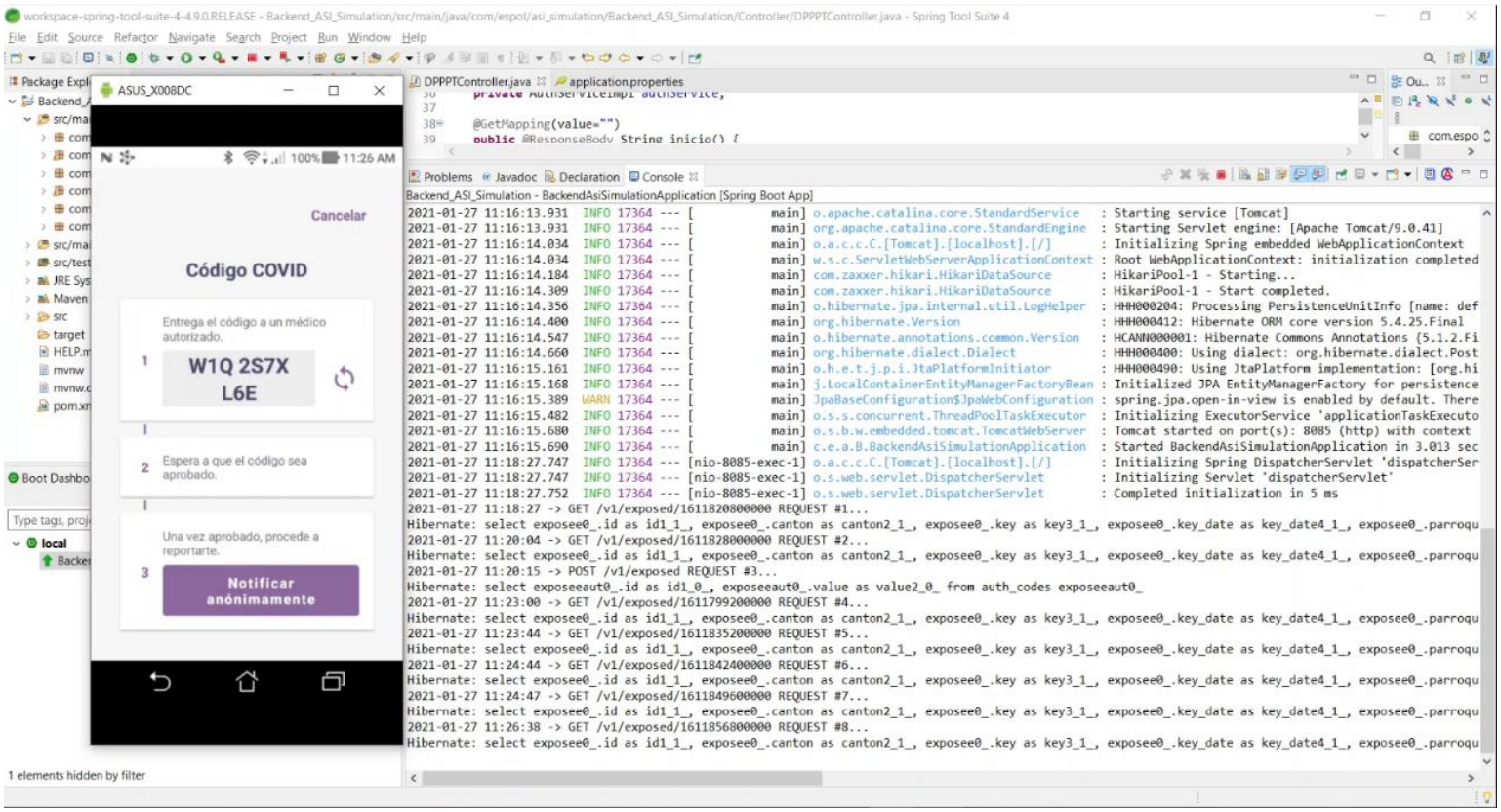


Resultados: Comunicación con el servidor

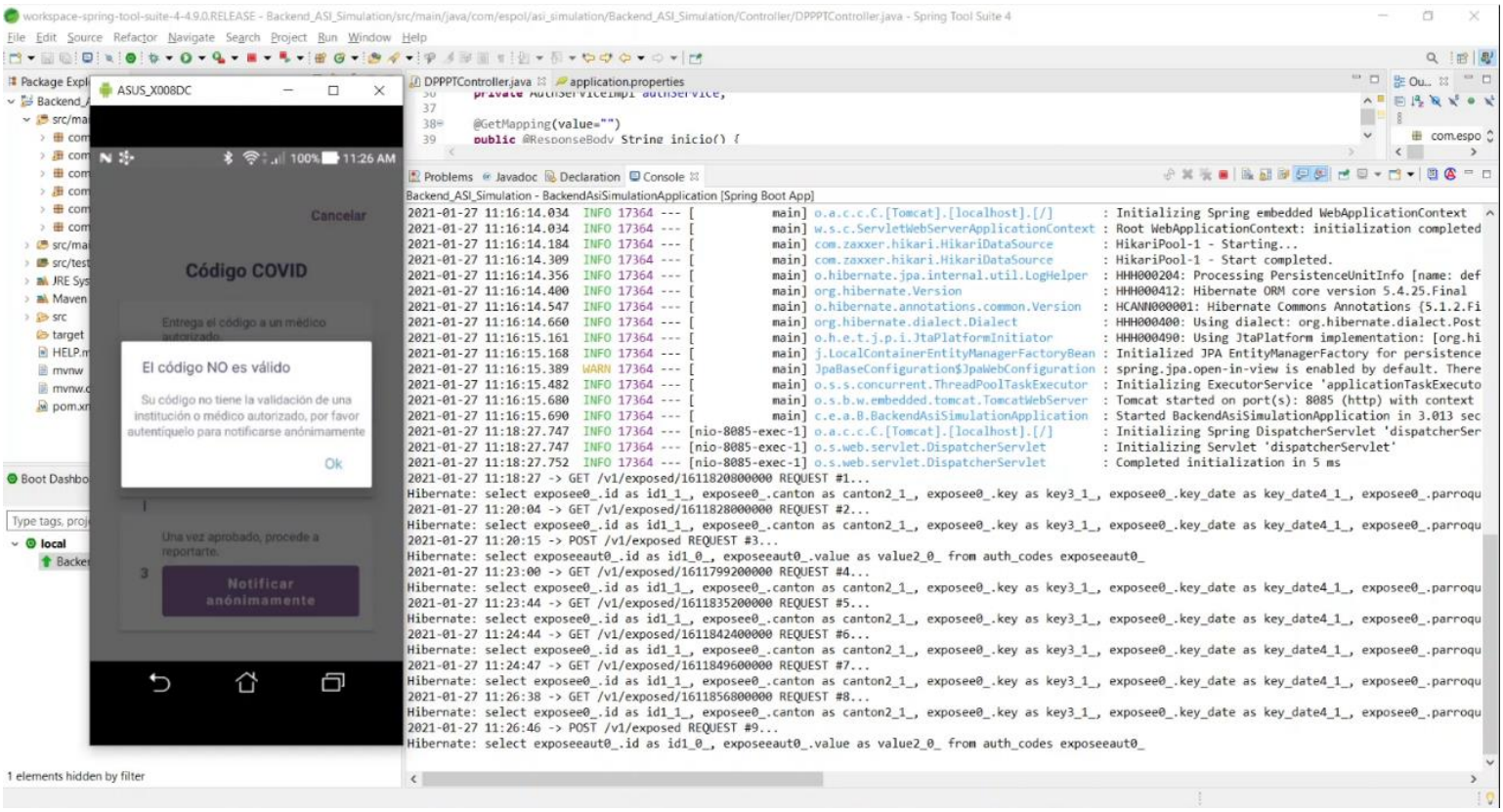
La siguiente captura muestra el primer dispositivo junto con el programa Spring Tool Suite, donde se desplegó el servidor local.



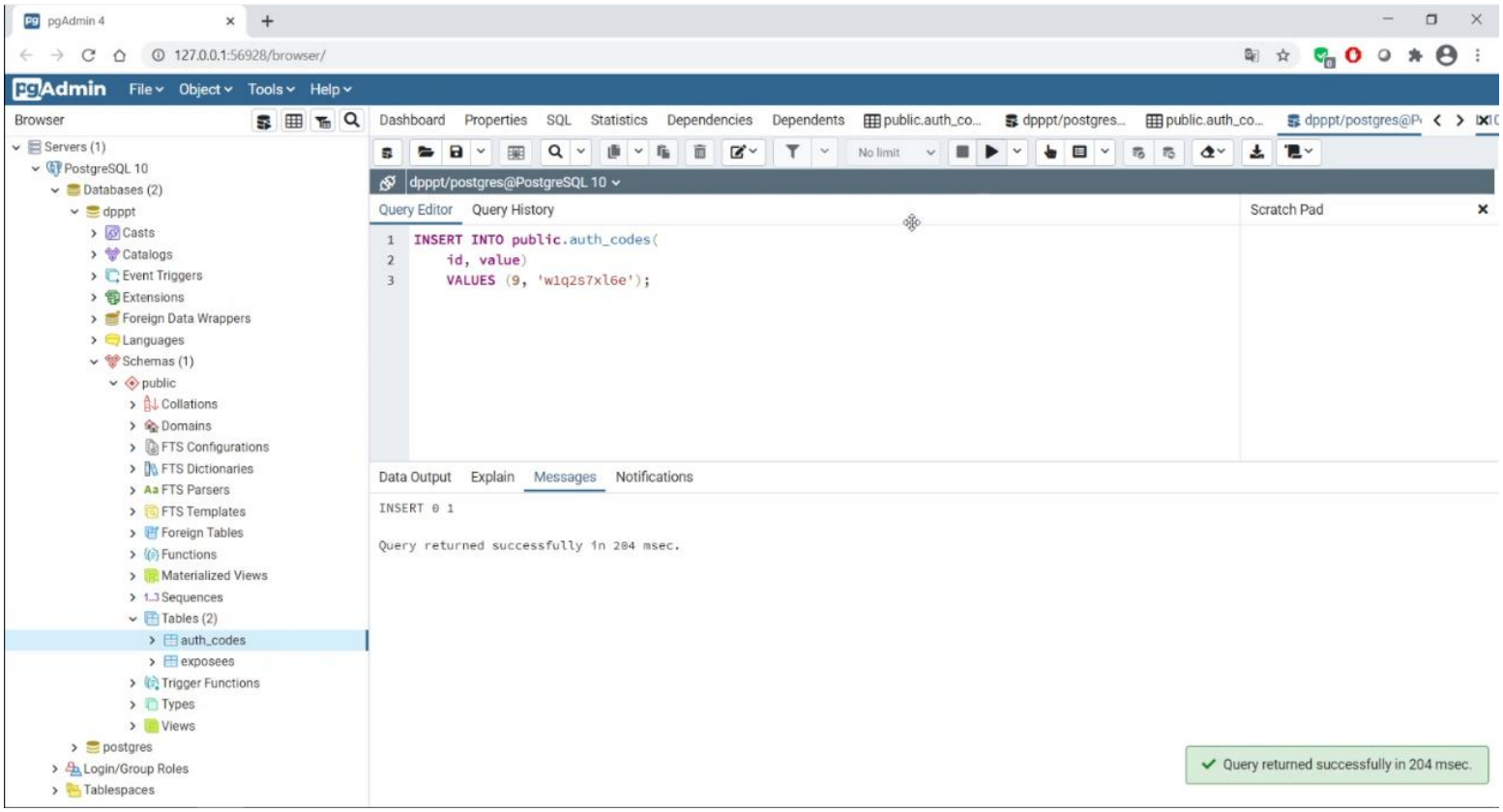
Aquí se usa la opción para reportarse como COVID positivo, donde también se destaca el código *W1Q2S7XL6E*, el cual debe ser ingresado en la base de datos.



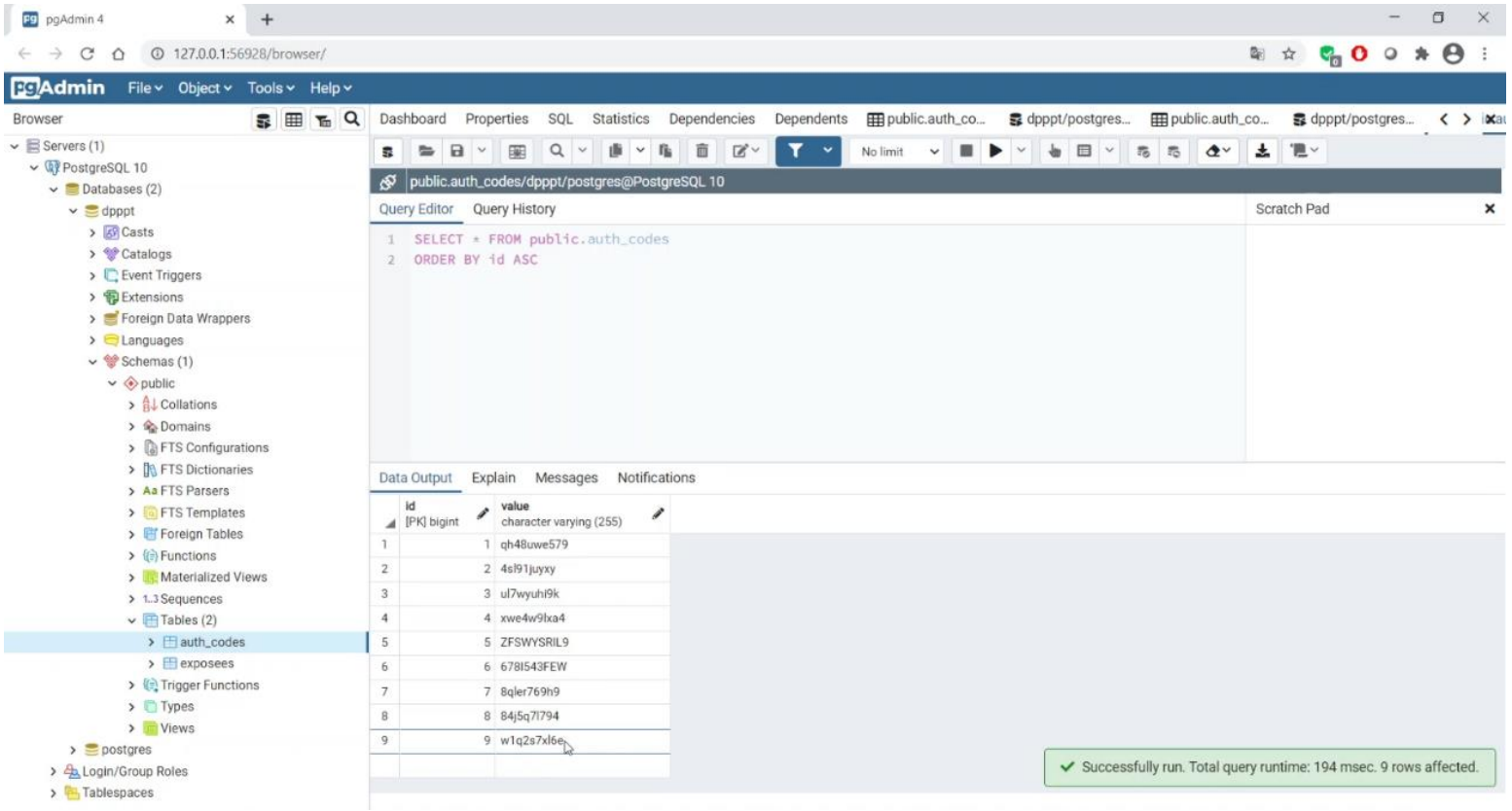
Al presionar el botón *Notificar anónimamente*, el servidor responde que el código NO es válido, debido a que aún no se ha registro el código COVID que se mencionó anteriormente.



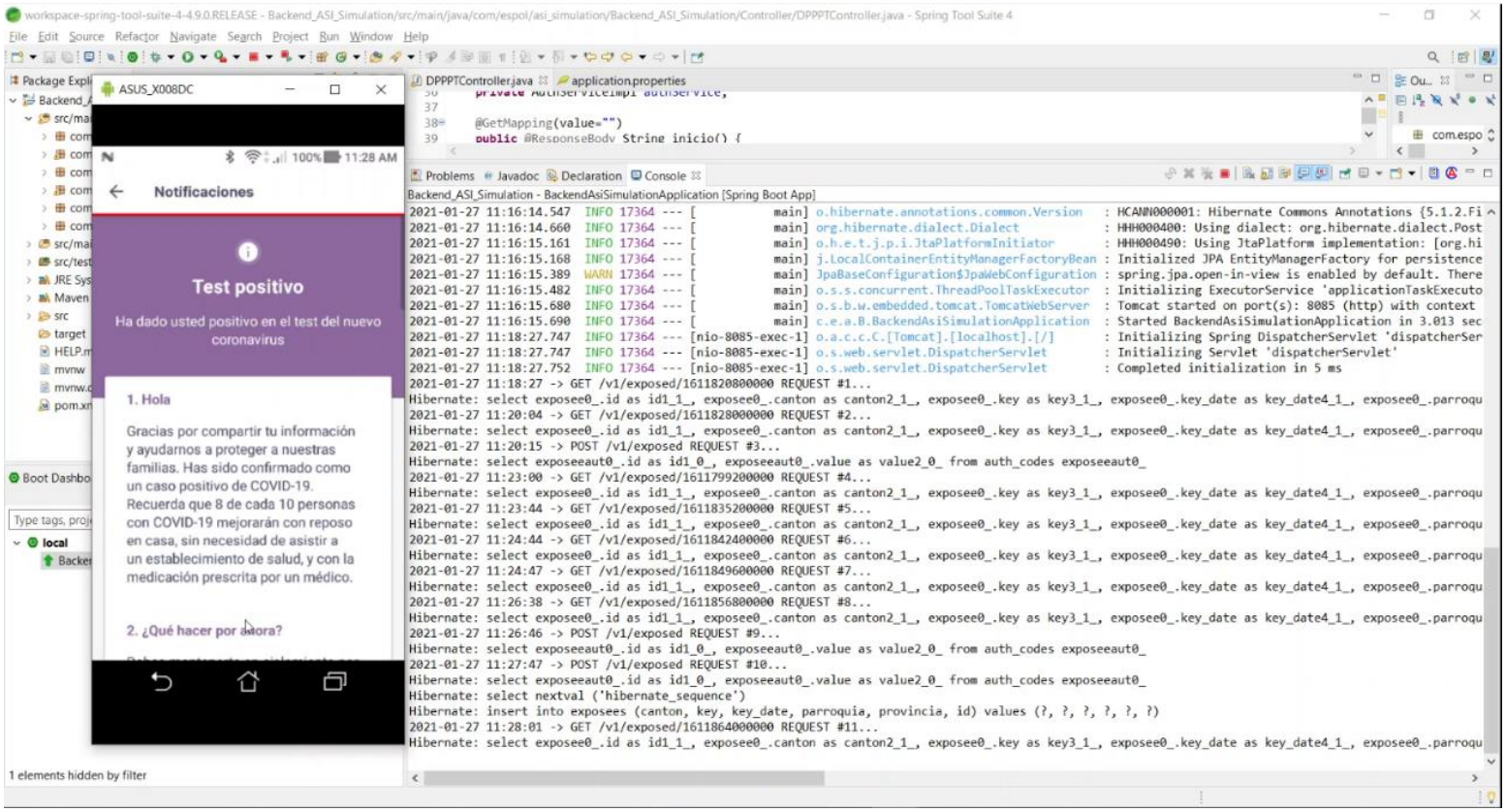
Para el registro del código se utiliza la interfaz web pgAdmin, y en la siguiente imagen se observa el query ingresado en la tabla auth_codes.



Se consultan todos los valores de la tabla y en la novena posición se visualiza el código correctamente ingresado, con lo cual el usuario ya podrá reportarse.



Luego se repite el proceso y esta vez sí responde favorablemente el servidor y aparece un mensaje de test positivo.



Finalmente, se observa que en el segundo dispositivo llega la notificación de posible contagio.