# PROTOCOLO DE PRUEBAS DE BTS Y CDR-s

Dirección de Antisecuestro y Antiextorsión



## 1. Objetivo

Adelantar pruebas de concepto de dispositivos que permitan recolectar información de BTS o antenas de telefonía móvil, IN SITU y vecinas de un sector definido y el posterior análisis temporal de la metadata colectada, mediante patrones de correlación que permita identificar eventos, selección de fechas específicas, visualización de movimientos de transacciones u ocurrencia de hechos, entre otros

## 2. Objetivos Específicos

2.1. Realizar pruebas, en escenarios rurales y urbanos, donde se colecte información de las BTS o antenas de telefonía móvil, inventario de celdas sobre redes de telefonía celular en tecnología 2G (GSM), 3G (UMTS/HSDPA/HSPA+), 4G/4.5G (LTE) y 5G (NR/SA/NSA), de los proveedores de servicios en cobertura, simulando o recreando la escena o lugar de los hechos, donde se visibilizarán datos específicos como Soporte para múltiples tecnologías de red: soporte para múltiples tecnologías de red autorizadas para Colombia.

2.2. Verificar la administración, procesamiento y tratamiento de datos colectados, con su respectivo informe final.

2.3. Validar el análisis de la información colectada para solicitar a los operadores lo CDRs, donde se genere informes de Policía Judicial. Como el formato FPJ 11

2.4. Realizar verificación de análisis de METADA – entregada por los operadores, mediante software que realice correlación y líneas de tiempo..

## 3. Requisitos Específicos hardware

### 3.1. Información técnica de entrega del dispositivo

Tipo de Red: Indica la tecnología de conexión actual del dispositivo, GSM, HSDPA, CDMA, LTE, etc.).
CELL ID (Identificador de Celda)
Proporciona datos de la celda de servicio activa, incluyendo el operador móvil
Registra el historial de celdas por las que ha pasado el dispositivo.
MCC (Código de País Móvil) Código único de 3 dígitos asignado a cada país.
MNC (Código de Red Móvil) Código de 2 o 3 dígitos que identifica al operador dentro de un país.
LAC (Código de Área de Localización), Divide la red en zonas geográficas para gestionar llamadas y datos.
NODE (Controlador de Red) 3G: Muestra el ID del Radio Network Controller (RNC) que gestiona la celda.

4G: Refleja el eNodeB ID (equivalente a la estación base en LTE).
CID (Cell ID) Número único asignado a la torre o antena a la que está conectado el dispositivo.
eNodeB En redes 4G, es el nodo que conecta los dispositivos móviles con la red central.

Banda de Frecuencia

- Bandas GSM (2G): 850/900/1800/1900 MHz
- Bandas WCDMA (3G): 850/900/1900/2100 MHz
- Bandas LTE (4G): B1/B2/B3/B4/B5/B7/B8/B12/B13/B20/B28/B66
- Capacidad de escaneo simultáneo en múltiples bandas
- Compatible con operadores nacionales: Claro, Tigo, WOM, Movistar
- Interfaz de comunicación serial de alta velocidad
- Voltaje de operación: 3.3V - 4.2V
- Dispositivo dedicado para redes 5G
- Bandas Sub-6 GHz: n1/n2/n3/n5/n7/n8/n20/n28/n38/n41/n66/n71/n77/n78/n79
- Soporte para 5G NSA (Non-Standalone) y SA (Standalone)
- Compatible con todos los operadores nacionales con cobertura 5G
- Interfaz de comunicación de alta velocidad).

**Tipo de Tecnología**

Ubicación (Latitud/Longitud) Coordenadas geográficas en formato decimal, obtenidas mediante GPS

**Velocidad y Precisión:**

Velocidad: Movimiento del dispositivo en km/h.
Precisión: Margen de error de la ubicación

**Roaming**

Indica si el dispositivo está usando la infraestructura de otro operador

### 3.2 Verificaciones de autenticidad y viabilidad

- Moden celular habilitados para Colombia, estén habilitados o certificados Comisión de Regulación de Comunicaciones de Colombia.
- Que el inventario de antenas genere los respectivos Hash 256 y 512,

para garantizar la autenticidad de las acciones realizada en campo o lugar de los hechos.

- Que genere informes de Policía Judicial, donde realiza el inventario de antenas titulares y vecinas.
- Que el hardware especializado tenga un programa de garantías y soporte.
- Que el hardware especializado tenga un programa de mantenimientos preventivos y calibración.
- Que el sistema genere los diferentes parámetros técnicos de lectura de la información necesaria para realizar el inventario de antenas y acrónimos especiales del operador celular como CELL ID, LAC entre otros descritos a continuación.

## PRUEBA DE CAMPO DISPOSITIVO DE INVENTARIO Y ANÁLISIS DE INFORMACIÓN DE BTS Y CDRS

01 La solución señalizara con una aproximación de la antena o BTS, las celdas más cercanas con sus diferentes potencias de RSSI y RSCP, RSRQ, SNR, ARFCN, Timing Advance (TA), y graficara en un sistema de mapa en los dos escenarios.

02 La solución de análisis de BTS y CDR-s, en la tecnología 2G (GSM) de los diferentes operadores celulares (Claro, Tigo, Movistar) con el fin de verificar el RSSI (Señal) por cada BTS DBM y su efectividad y ubicación en un mapa en tiempo real.

03 La solución de análisis de BTS y CDR-s, debe llegar a ubicar antenas en tecnología 3G (UMTS) en los diferentes operadores celulares (Claro, Wom, Tigo, Movistar) con el fin de verificar la potencia por cada BTS su efectividad y señalizándola en un mapa en ubicación real, de igual manera la información de la CELL ID en datos

04 La solución de análisis de BTS y CDR-s, debe tener la capacidad de ubicar antenas en tecnología 4G (LTE) en los diferentes operadores celulares (Claro, Tigo, Movistar, Wom y Avantel) con el fin de verificar la potencia por cada BTS su efectividad y señalizándola en un mapa en ubicación real.

05 La solución de análisis de BTS y CDR-s, debe tener la capacidad de ubicar antenas en tecnología 5G (SA/NSA) en los diferentes operadores celulares (Claro, Tigo, Movistar, Wom y Avantel) con el fin de verificar la potencia por cada BTS su efectividad y señalizándola en un mapa en ubicación real. Cabe resaltar que en el caso de NSA debe contar con la capacidad de indicar al usuario, dado las características compartidas con redes 4G.

06 La solución de análisis de BTS y CDR-s, de BTS, debe señalizar las antenas

vecinas, indicando su nivel de señal en RSSI, LAC y CELLID.

07 La solución de análisis de BTS permite visualizar de forma gráfica el estado de la potencia actual y comparativa a lo largo del tiempo de la celda principal de conexión según sea la red.

08 La solución de análisis de BTS y CDR-s, debe tener la capacidad de analizar información suministrada por los operadores móviles, con el fin de interpretar el caso y obtener números objetivos.

09 La solución de análisis de BTS y CDR-s, en su inventario de antenas debe ser almacenado en archivos digitales que serán acompañados de su respectivo hash en formato sha256 y/o sha512. Lo anterior, con el propósito de conservar la cadena de custodia y garantizar el principio de mismidad de la evidencia colectada y garantizar la no alteración de la información tomada en campo por parte del funcionario que opere la solución tecnológica.

10 La solución de análisis de BTS y CDR-s, de manera automática debe generar el formato de investigador de campo FPJ-11, donde se presenta el inventario de antenas identificadas en las diligencias de campo en el lugar del crimen o sitios de interés. Este informe FPJ-11 tiene como propósito, permitir al fiscal encargado del caso solicitar ante un juez de garantías la búsqueda selectiva en base de datos de los CDRs (Registro detallado de llamadas) a cada uno de los operadores celulares identificados en las diligencias.

11 La solución de análisis de BTS y CDR-s el módulo de análisis de CDRs debe orientar su investigación encontrando patrones de correlación de actividad de telefonía celular. La solución tecnológica permite realizar gráficos y líneas de tiempo, que permiten tener una apreciación de la posible participación de teléfonos móviles en un determinado lugar de los hechos.

12 El sistema de análisis de BTS y CDRs debe normalizar los registros de llamadas (Call Detail Records) proporcionados por el operador, asegurando la coherencia y uniformidad de los datos. Esto implica

Homologación de formatos, Validar que los datos clave (CELL ID, timestamps entre otros), Vincular cada CDR con la BTS correspondiente mediante identificadores únicos, garantizar que los CDRs estandarizados sean compatibles con herramientas de análisis posteriores

Crear una base de datos consolidada donde los CDRs y la información de celdas (BTS) puedan cruzarse con precisión para estudios de tráfico, optimización de red o geolocalización.

## PROCEDIMIENTO DE PRUEBAS DE CONCEPTO
## (funcionamiento y manejo del dispositivo)

| Item | CASO DE PRUEBA | CUMPLE | | OBSERVACIONES |
|---|---|---|---|---|
| | | SI | NO | |
| 1 | El sistema arranca exitosamente y esta encendido todos los dispositivos de forma automática. | | | |
| 2 | Visualización de carga de baterías. | | | |
| 3 | Encendido de los dispositivos de telefonía. (16 o según el caso) | | | |
| 4 | Muestra el Nombre del Operador del proveedor de servicios en MCC y MNC. Muestra el MNC - Código de red móvil – (es un código de 2 o 3 dígitos y es específico para cada país operador en el país) | | | |
| 5 | Muestra el LAC y TAC, código de área de ubicación – (la red está dividida por áreas de ubicación, en las que el suscriptor es localizado en todas las celdas simultáneamente. LAC es el Código del area actual). | | | |
| 6 | Muestra el CID: (que es el código de la CELLI ID de la celda de servicio actual). | | | |
| 7 | Muestra el PCI / PSC / BSIC - PCI en 4G, PSC en 3G y BSIC en 2G para la celda de servicio actual. | | | |
| 8 | Muestra el F - Número de canal de frecuencia ARFCN | | | |
| 9 | Muestra el B - banda de frecuencia (Uxx para 3G, Lxx para LTE) | | | |
| 10 | Muestra el TA - avance de tiempo - para 2G y 4G | | | |
| 11 | Muestra el Tipo - el modo de tecnología de red (como GPRS, EDGE en 2G o UMTS, HSPA, WCDMA, etc. … En 3G,4G Y 5G) | | | |
| 12 | Muestra el - NIVEL - la intensidad de la señal actual en dBm. Para diferentes tecnologías, el título es diferente: RXLEV para 2G, RSCP para 3G y RSRP para 4G. | | | |
| 13. | Muestra el - QUAL: la calidad de la señal de la red. Para las diferentes tecnologías, el título es diferente: RXQUAL para 2G, ECNO para 3G y RSRQ para 4G. La mayoría de los teléfonos no informan este valor. Solo varios teléfonos informan ECNO y tal vez ningún teléfono informa RXQUAL. | | | |
| 14. | Muestra el - SNR - relación señal / ruido. Se mide solo en LTE. | | | |
| 15. | Muestra el - CQI - indicador de calidad del canal. Se mide solo en 4G. | | | |
| 16.. | Muestra – Longitud latitud de la ubicación actual en formato decimal | | | |
| 17. | Muestra la Velocidad: actual en kmph de la recolección de información | | | |

| | | | | |
|---|---|---|---|---|
| 18. | Muestra la - Precisión: con la que se determina la ubicación. La determinación de la ubicación basada en GPS o sistemas similares satelitales. | | | |
| 19. | Muestra la - Altura - la diferencia entre los valores de Altitud y Tierra | | | |
| 20. | Muestra - UL: la velocidad de transferencia de datos de enlace ascendente actual en kbps | | | |
| 21. | Muestra - DL - la velocidad de transferencia de datos de enlace descendente actual en kbps | | | |
| 22. | Muestra - Datos - la red de datos utilizada - Red móvil o WiFi | | | |
| 23. | Muestra la - Tabla del historial de la celda de servicio: esta tabla muestra el registro histórico de los cambios de la celda de servicio con la hora del cambio y el nivel en el que ocurrió este cambio. La tabla también muestra el tiempo de servicio celular, que es útil para detectar re-selecciones celulares frecuentes y la falta de células dominantes. | | | |
| 24. | Identifica celdas y Mapeo de la red de telefonía celular, para operación en Tecnologías 2G (GSM), 3G - UMTS/HSDPA/HSPA+), 4G/4.5G (LTE) y 5G(NR/SA/NSA). | | | |
| 25. | Identifica y captura celdas vecinas en el servicio 2G / 3G / 4G / 5G | | | |
| 26. | Gráfico con niveles de celdas y celdas vecinas | | | |
| 27. | Grabación y exportación en mediciones en archivos de registro (formato de TXT y KML) | | | |
| 28. | Cuenta con la opción de Limpiar la vista - si hay muchos puntos en un recorrido, para la vista del mapa y toma de evidencias. | | | |
| 29. | Muestra el SDK de Android - el número de versión del sistema operativo Android | | | |
| 30. | Cuenta con una ventana de información principal de las celdas de servicio en un formato cómodo y con letras grandes que resuma los resultados del análisis. | | | |
| 31. | Permite mediante una única simcard obtener los parámetros del canal de voz y del canal de datos (eNB – CellID, según sea la red) | | | |
| 32. | Se pueden cargar o Mostrar sitios: requiere tener un archivo con información de celdas de BTS. | | | |

| | | | | |
|---|---|---|---|---|
| 33. | Se puede Usar una base de datos: cuando está activado la herramienta se utilizará la carga de celdas de la base de datos en lugar de cargar celdas del archivo de celdas. La carga de la celda de la base de datos es mucho más rápida y eficiente. | | | |
| 34. | Se puede Ordenar por distancia la base de datos de las celdas BTS - cuando está encendido garantizará mostrar la celda más cercana. | | | |
| 35. | Presenta la línea de servicio: muestra una línea entre la ubicación actual y la ubicación de la celda de servicio | | | |
| 36. | Muestra códigos de celda. | | | |
| 37. | Muestra los puntos para las celdas: al marcar esto, se dibujarán puntos en lugar de líneas para las celdas, lo que mejora el rendimiento del mapa. | | | |
| 38. | Parametriza el máximo de celdas visualizadas: este es el número máximo de celdas que se visualizarán de todas las celdas que se cargan en la memoria. Si desea aumentar este número, puede usar las dos funciones siguientes para lograr un mejor rendimiento del mapa. | | | |
| 39. | Agrega celdas desconocidas: cuando esta opción está activa, las celdas nuevas se agregan automáticamente al archivo de celdas. la aplicación creará un nuevo archivo de celda y cuando el registro esté activado, comenzará a llenarlo con nuevas celdas. | | | |
| 40. | Presenta el código de las celdas vecinas: cuando se marca, el nombre de la celda vecina, la distancia y el rumbo se mostrarán en la tabla Vecinos (requiere información 3G PSC / 4G PCI en el archivo de celda) | | | |
| 41. | Muestra líneas de celdas vecinas: cuando se marca, las líneas de celdas vecinas se visualizarán en el mapa | | | |
| 42. | Toma color de celda: elija el color de celda según TECH, CELLID o PCI / PSC / BSIC. | | | |
| 43. | Muestra valores HEX: cuando se muestran los valores hexadecimales para cellid. | | | |
| 44. | Cuenta con la calibración de las diferentes redes 2G,3G,4G Y 5G para obtener una mejor obtención de los Datos. | | | |
| 45. | Permite el ingreso de puntos de referencia para la recolección de información. | | | |
| 46. | Mantiene la conservación de la extracción digital datos mediante (HASH-SHA256 y SHA 512), preservando la mismidad. | | | |