MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
INSPECCIÓN GENERAL
OFICINA CONTROL DISCIPLINARIO INTERNO INSTRUCCIÓN No. 9

NOTIFICACIÓN POR ESTADO:

Fecha del estado:	25 de julio de 2024
Radicado del proceso	EE-DECAL-2024-46
Quejoso / Informante:	MARÍA José Loaiza González
Investigado (s):	Patrullero CRISTIAN RODRIGO GÓMEZ ABREO
Documento de Identidad:	1.054.557.758 de la Dorada
Fecha y lugar de los hechos	Aránzazu Caldas, enero 2024
Fecha del Informe laboratorio	24 de julio del 2024
Contenido	**Informe Investigador de laboratorio, extracción de información equipo terminal móvil marca SAMSUNG**
Hora de fijación del estado	08:00 horas (Comienzo de la primera hora hábil)
Término de fijación del estado:	Un (1) día, para notificar a los sujetos procesales

Se **FIJA** el presente estado a los 25 días del mes de julio del año 2024, siendo las 08:00 horas en la página web https://www.policia.gov.co/notificaciones-por-estado tal como lo dispone la Ley 1952 de 2019, en su artículo 123 y 125, por medio de la cual se expide el Código General Disciplinario y se dictan otras disposiciones.

Subintendente **ROBINSON HERNÁN LARGO**
Sustanciador de Procesos Disciplinarios y/o Penales.

Se **DESFIJA** el presente estado hoy 25 de julio del año 2024, a las 18:00 horas.

Hace Constar:

Subintendente **ROBINSON HERNÁN LARGO**
Sustanciador de Procesos Disciplinarios y/o Penales.

POLICÍA NACIONAL

Entidad	Radicado Interno	Departamento	Municipio	entidad	Unidad Receptora	Año	Consecutivo
		0 0	0 0 0	0 0	0 0 0 0 0	2 0 2 4	0 0 0 4 6

Número Único de Noticia Criminal

INFORME INVESTIGADOR DE LABORATORIO – FPJ - 13

Este informe será rendido por la Policía Judicial

Departamento	Caldas	Municipio	Manizales	Fecha	2024	07	24	Hora	1	0	0	0

Conforme a lo establecido en los artículos 210, 254 255, 257, 261,275 y 406 de la Ley 906 de 2004 C.P.P, me permito rendir el siguiente informe, bajo la gravedad de juramento, se rinde el siguiente informe.

1. IDENTIFICACIÓN DEL INFORME

Informe de Laboratorio N° 198 /2024 y Orden de Trabajo N° 202401280.

Grupo Regional de Policía Científica y Criminalística N° 3.
Laboratorio de Informática Forense
Carrera 25 N° 32 – 50 barrio Linares
Manizales – Caldas.

Rdo SI Hernan Largo Robinson 24-07-2024 11:20 Horas

2. DESTINO DEL INFORME

Teniente
JAIME ALBERTO OROZCO PERDOMO
Jefe Oficina Control Disciplinario Interno de Instrucción No 9 DECAL
Carrera 25 número 32 – 50.
Manizales - Caldas.

3. ESTUDIO SOLICITADO

Dar cumplimiento al Auto EE-DECAL-2024-46 de fecha 04/06/2024 emitida por la Oficina Control Disciplinario Interno de Instrucción No 9 DECAL, teniente. JAIME ALBERTO OROZCO PERDOMO; Comunicación Oficial, radicado GS-2024-063951- DECAL de fecha 24/06/2024, suscrita por el señor Subintendente ROBINSON HERNAN LARGO, donde solicitan:

"PERICIALES*:*

Una vez se agote la diligencia de declaración, de la señora auxiliar de policía María José Loaiza, González y si esta lo autoriza, Enviar el equipo celular al Grupo Regional de Policía Científica y Criminalística Nro 3 con el fin de efectuar la extracción de la conversación y la imagen de la parte intima que se relaciona en la queja."

4. DESCRIPCIÓN DE LOS ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FÍSICA RECIBIDOS PARA ESTUDIO

4.1 Evidencia N° 1. Contiene los siguientes elementos:

4.1.1 Evidencia N° 1.1 Un (01) equipo terminal móvil marca SAMSUNG, modelo SM-A047M, color NEGRO, IMEI[1] Físico: 359472/81/133050/3, (01) batería interna.

[1] IMEI: Identidad Internacional de Equipo Móvil

4.1.2 **Evidencia N° 1.2.** Una (01) tarjeta SIM color rojo, con el logotipo de la empresa de comunicaciones CLARO, ICCID[2] Físico No 57101602303773136, la cual se encontraba al interior del teléfono celular relacionado en el ítem 4.1.1.

4.1.3 **Evidencia N° 1.3.** Una (01) tarjeta MICROSD, sin marca, capacidad de almacenamiento 2GB, serie 1327CQ8302P, la cual se encontraba dentro de la evidencia 4.1.1.

5 DESCRIPCIÓN Y EXPLICACIÓN DE LOS PRINCIPIOS, MÉTODOS Y PROCEDIMIENTOS TÉCNICOS UTILIZADOS

5.1 EXPLICACIÓN DEL PRINCIPIO O PRINCIPIOS TÉCNICOS – CIENTÍFICOS APLICADOS (INFORME SOBRE EL GRADO DE ACEPTACIÓN POR LA COMUNIDAD CIENTÍFICA).

Principio de Disponibilidad: Cuando la información es accesible a los usuarios autorizados en el momento de requerirla.

Principio de no Repudiación: Cuando la información involucrada en un evento corresponde a quien participa en el mismo, quien no podrá desconocer su intervención en dicho evento.

Principio de Integridad: Cuando se garantiza que la información es exacta y completa, no se modifica desde el momento de su creación y se almacena en un formato que asegura la exactitud de la información original.

Observancia: Cuando se lleva el registro de los eventos importantes.

5.2 DESCRIPCIÓN DE LOS MÉTODOS O PROCEDIMIENTOS UTILIZADOS

Se aplican los procedimientos establecidos por la Policía Nacional:

2DC-PR 0002 Tratamiento y análisis de la evidencia digital.
2DC-PR 0027 Extracción de información a equipos terminales móviles.
2DC-PR 0033 Realizar imágenes forenses.

6. ACEPTACIÓN DE LOS PRINCIPIOS, MÉTODOS O PROCEDIMIENTOS POR LA COMUNIDAD TÉCNICO-CIENTÍFICA.

Los procedimientos empleados para realizar la identificación, preservación, recolección y análisis de la información almacenada en dispositivos de almacenamiento digital, gozan de total aceptación por parte de la comunidad técnico científica, al tratarse de actividades debidamente reconocidas y avaladas en la realización de los diferentes análisis forenses de computadoras y dispositivos electrónicos de almacenamiento de datos, que se efectúan a nivel mundial por parte de expertos en esta área, en donde apoyados en herramientas de software y hardware especializado, se lleva a la práctica un conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento de la información almacenada en un medio digital preservando la integridad de la evidencia.

7. EQUIPOS E INSTRUMENTOS EMPLEADOS Y SU ESTADO DE MANTENIMIENTO

7.1 UFED 4 PC de Cellebrite versión 10.2.0.359 Se trata de una herramienta utilizada para la extracción de datos forenses en teléfonos celulares. El sistema UFED de CelleBrite es compatible con las tecnologías CDMA, GSM, IDEN y TDMA, así como con todos los operadores de telefonía celular incluidos teléfonos inteligentes, asistentes digitales personales y (PDA).

7.2 UFED Physical Analyzer versión 10.2.100.248: este programa es una herramienta forense que se utiliza para la decodificación, análisis y generación de informe de la información obtenida por la herramienta forense UFED 4 PC.

[2] ICCID: Identificador Internacional de la Tarjeta de Circuitos

7.3 Programa FTK® IMAGER versión 4.5.0.3, este programa es una herramienta forense que se utiliza para crear copias exactas o imagen forense de datos de computadoras y otros dispositivos de almacenamiento, sin realizar ningún cambio a la evidencia original, de igual forma podemos autenticar la información extraída de las evidencias analizadas mediante sumas de verificación[3] utilizando la función Hash[4] MD5[5] y SHA1[6].

7.4 Una estación de cómputo marca HP en buen estado de funcionamiento.

7.5 Sistema Operativo Microsoft Windows 11, Sistema Operativo de 64 Bits y Paquete de Microsoft Office 2019.

7.6 Cámara fotográfica marca Canon PowerShot A650 IS, Serial No. 5026103482, tipo digital, lente fijo, zoom óptico 6X tarjeta almacenamiento SD Marca KINGSTON de 4 GB y flash incorporado, con baterías recargables de 2700 mAh marca SONY de 1.2 V en buen estado de funcionamiento.

7.7 Programa NERO Express Versión 12.0.20.0, el cual se trata de un software de grabación de discos para Windows, con el que es posible grabar datos, contenido multimedia, copiar discos o extraer CDs de audio.

El hardware y software utilizado para el análisis de los medios de almacenamiento digital, se encuentra en buen estado de funcionamiento al momento de realizar el procedimiento o peritaje de Informática Forense.

8. RESULTADOS

8.1 Se solicitan los EMP y EF a la bodega transitoria de evidencias del Grupo Regional de Policía Científica y Criminalística N° 03, realizando el registro de continuidad de la cadena de custodia.

8.2 Se extraen los EMP y EF de su contenedor y se verifican que los elementos sean los mismos que se encuentran descritos en el rótulo correspondiente.

8.3 Se verifican la integridad y el estado en general del EMP y EF, allegado al laboratorio mediante la observación del embalaje, rotulo y cadena de custodia, realizando la respectiva constancia mediante registro fotográfico por parte del perito, así como de los números de identificación del dispositivo a analizar.

8.4 Dentro de la preparación de las herramientas forenses para el procedimiento de análisis se procede a realizar un borrado seguro previo a la unidad de almacenamiento correspondiente a la estación forense donde se realizar el análisis, posteriormente se realiza la instalación de los programas relacionados en el numeral **7.**

8.5 Se procede a realizar la extracción forense de la información contenida en las evidencias relacionadas en los ítems, **4.1.1, 4.1.2 y 4.1.3,** utilizando la herramienta forense (**UFED 4 PC - CELLEBRITE**), empleando la opción "Extracción Lógica[7], Extracción Física[8], Extracción del Sistema de Archivos[9]" o "Extracción de Datos Desde SIM", según el equipo celular, tarjeta SIM o MicroSD objeto de análisis, y se genera un archivo de extensión .UFDX para cada extracción realizada.

8.6 Empleando el software UFED Physical Analyzer se procede a realizar la decodificación, análisis y generación de informe de la información contenida, en los archivos .UFDX adquirido de las evidencias relacionadas en los ítems, **4.1.1, 4.1.2 y 4.1.3,** seleccionando el tipo de contenido a extraer según lo solicitado en el numeral **4.**

8.7 Con el fin de dar respuesta a lo solicitado en el presente análisis pericial, por medio del auto y comunicación oficial descritos en el numeral 3, se procese a configurar en la herramienta forense UFED Physical Analyzer, como criterios de búsqueda, la red mensajería instantánea WhatsApp y la información trasmitida (chats y contenido multimedia) por esta red entre el 09/01/2024 y 12/01/2024, estos resultados de búsqueda son los que se exportan para ser analizados por la autoridad solicitante.

3 Suma de verificación: Procedimiento matemático que mediante el empleo de un algoritmo permite identificar un archivo con valor único, este valor se calcula sobre el contenido del archivo y no sobre el nombre del mismo, mediante el uso de una función específica MD5, SHA1, entre otros. **MD5:** Message Digest algorihm 5. **SHA1:** Secure hash algorithm 1.
4 Se refiere a una función o método para generar claves o llaves que represente de manera univoca a un documento, registró, archivo etc... Un hash es el resultado de dicha función o algoritmo.
5 Acrónimo de Message-Digest Algorithm 5, algoritmo de resumen de mensaje 5 empelado para crear firmas digitales y verificar la integridad del archivo
6 Es una función hash criptográfica que toma una entrada y produce un valor hash de 160 bits conocido como resumen del mensaje.
7 Extracción Lógica: se trata de extraer la información que tiene activa el equipo de comunicación
8 Extracción Física: Es una copia bit a bit de la información activa y eliminada del dispositivo
9 Extracción del Sistema de Archivos: se trata de extraer la información activa y eliminada dependiendo del modelo del equipo.

8.8 Empleando el Programa FTK Imager se autentica la información exportada mediante sumas de verificación de tipo MD5 y SHA1 para garantizar la integridad de los archivos contenidos obteniendo una lista de archivo formato .XLSX o archivo ofimático de hoja o planilla de cálculo denominada: **SUMAS DE VERIFICACIÓN INFORMACION EXPORTADA 202400046.**

9. INTERPRETACIÓN DE RESULTADOS / CONCLUSIONES

Como resultado de la extracción de información realizada a los EMP – EF relacionados en el numeral **4** y teniendo en cuenta lo solicitado en auto y comunicación oficial descritos en el numeral **3,** se obtiene la siguiente información:

9.1 Para la **Evidencia N° 1.1,** Un (01) equipo terminal móvil marca SAMSUNG, modelo SM-A047M, relacionado en el ítem **4.1.1,** teniendo en cuenta lo descrito en los ítems **8.5** y **8.6,** se procede a realizar la extracción forense de la información contenida en el mismo, empleando el dispositivo (**UFED 4PC de CELLEBRITE**) y utilizando la opción **(Extracción del Sistema de Archivos)**, se genera un reporte en archivo .PDF de nombre: **TELEFONO**, con la información obtenida, la cual se almacena en la ruta**INFORMACIÓN EXPORTADA\EVIDENCIA\TELEFONO**, del dispositivo de almacenamiento digital descrito en el numeral "11 ANEXOS" del presente informe investigador de laboratorio para ser verificado y valorado por el investigador del caso.

9.1.2 Con el fin de dar respuesta a lo solicitado en el presente análisis pericial, por medio del auto y comunicación oficial descritos en el numeral 3, se procese a configurar en la herramienta forense UFED Physical Analyzer, como criterios de búsqueda, la red mensajería instantánea WhatsApp y la información trasmitida (chats y contenido multimedia) por esta red entre el 09/01/2024 y 12/01/2024, estos resultados de búsqueda son los que se exportan para ser analizados por la autoridad solicitante.

9.2 Para la **Evidencia N° 1.2,** Una (01) tarjeta SIM color rojo, con el logotipo de la empresa de comunicaciones CLARO, ICCID Físico No. 57101602303773136, relacionada en el ítem **4.1.2,** teniendo en cuenta lo descrito en los ítems **8.5** y **8.6,** se procede a realizar la extracción forense de la información contenida en la misma, empleando el dispositivo **(UFED 4PC DE CELLEBRITE)** y utilizando la opción "Extracción de Datos Desde SIM", se genera un reporte en archivo .PDF de nombre: **Informe_Simcard** con la información extraída, obtenida, la cual se almacena en la ruta **\INFORMACIÓN EXPORTADA\EVIDENCIA1SIMCARD,** del dispositivo de almacenamiento digital descrito en el numeral "11 ANEXOS" del presente informe investigador de laboratorio para poder ser verificado y valorado por el investigador del caso.

Información del dispositivo (5)

⚠ Los eventos marcados en azul son para datos que no han sido extraídos del dispositivo.

#	Categoría	Nombre	Valor	Time	Eliminado	*
1	General	Model	SIM			
2	General	Vendor	SIM Card			
3	General	ICCID	89571016023037731369			
4	General	IMSI	732101637955159			
5	General	ACC	0x0200 = Class 9			

Contenido

Tipo	Incluido en el informe	Total
Contactos	2	2
Datos de SIM	27	27
Información del dispositivo	5	5

9.3 Para la **Evidencia N° 1.3,** Una (01) tarjeta MICROSD, sin marca, capacidad de almacenamiento 2GB, serie 1327CQ8302P, teniendo en cuenta lo descrito en los ítems **8.5** y **8.6,** se procede a extraer la información con el dispositivo **(UFED 4PC DE CELLEBRITE)**, utilizando la opción "**Extracción Sistema de archivos**", y se genera un reporte en archivo .PDF de nombre: **Informe_Microsd** con la información extraída, obtenida, la cual se almacena en la ruta **\INFORMACIÓN EXPORTADA\EVIDENCIA\MICROSD,** del dispositivo de almacenamiento digital descrito en el numeral "11 ANEXOS" del presente informe investigador de laboratorio para poder ser verificado y valorado por el investigador del caso.

Contenido

Tipo	Incluido en el informe	Total
Información del dispositivo	2	2
Cronograma	270	270
Vista Ubicaciones	51	51
Archivos de datos	432	432
Imágenes	323	323
Sonido	19	19
Texto	64	64
Vídeos	26	26

9.4 La información hallada como resultado del análisis forense es exportada y es conferida únicamente según los criterios de búsqueda solicitados por dicho despacho y lo soportado por las herramientas existentes actualmente en el Laboratorio de Informática Forense.

9.5 Se autentica la información empleando el programa FTK Imager, mediante sumas de verificación de tipo MD5 y SHA1 para garantizar la integridad de los archivos contenidos obteniendo un archivo de extensión .XLS, denominado **SUMAS DE VERIFICACIÓN INFORMACION EXPORTADA 202400046,** el cual se almacena en la capeta nombrada Información Exportada para poder ser analizada por el investigador del caso.

9.6 Se almacena la totalidad de la información extraída como resultado del análisis en Un (01) Disco BLU-RAY, sin marca, capacidad de almacenamiento 25 GB, el cual se anexan al presente Informe de Investigador de Laboratorio para poder ser valorada y analizada por el investigador del caso.

10.OBSERVACIONES

Los resultados de este Informe Pericial solo están relacionados con los Elementos Materiales Probatorio y Evidencia Física enviados para análisis descritos en numeral **4** del presente Informe Investigador de Laboratorio.

Adjunto al presente Informe de Investigador de Laboratorio, se hace entrega de los EMP – EF relacionados en el numeral **4** debidamente embalados, rotulados y con su respectiva cadena de custodia.

La información encontrada estará en custodia en almacenamiento digital, en el Laboratorio de Informática Forense por el lapso de (03) TRES MESES. Solicito muy respetuosamente a ese despacho en caso de ser necesario y de interés para la investigación se allegue solicitud por escrito de prórroga del almacenamiento por el mismo periodo de tiempo, toda vez que este laboratorio no cuenta con suficiente espacio de almacenamiento digital.

11.ANEXOS

Un (01) Disco BLU-RAY, sin marca, color blanco, capacidad de almacenamiento 25 GB, número de serie anillo interno LMA00307DE3035X22100315A, marcado con el manuscrito: **Información Exportada, Radicado No. 00000000000202400046,** elemento debidamente embalado, rotulado, sellado y sometido al protocolo de cadena de custodia.

Fijacion Fotografica

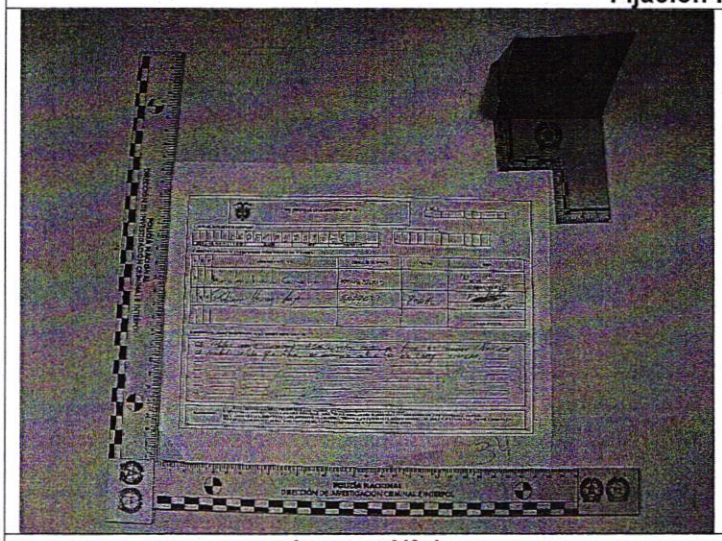

Imagen N° 1.

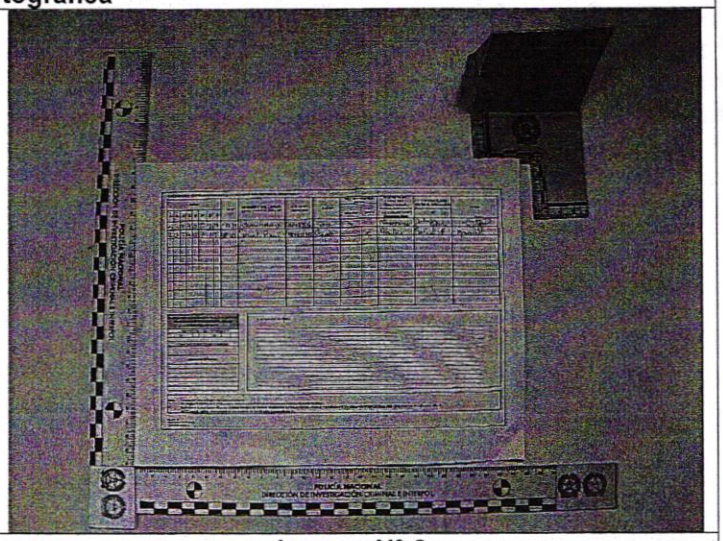

Imagen N° 2.

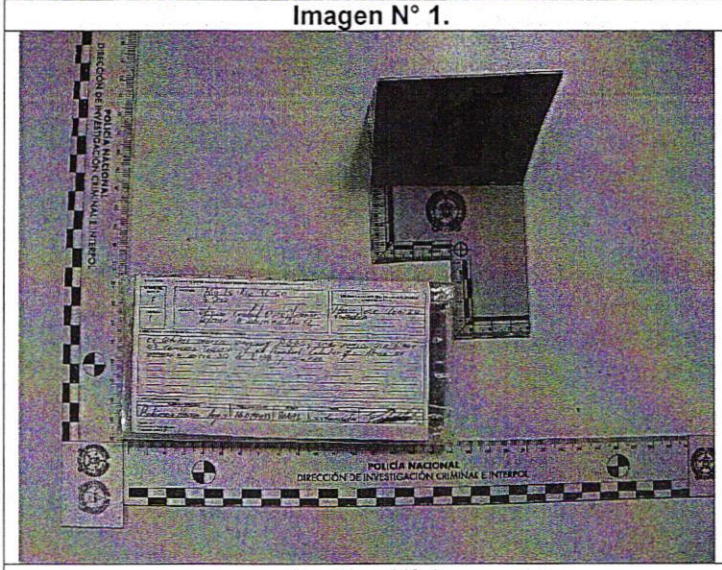

Imagen N° 3.

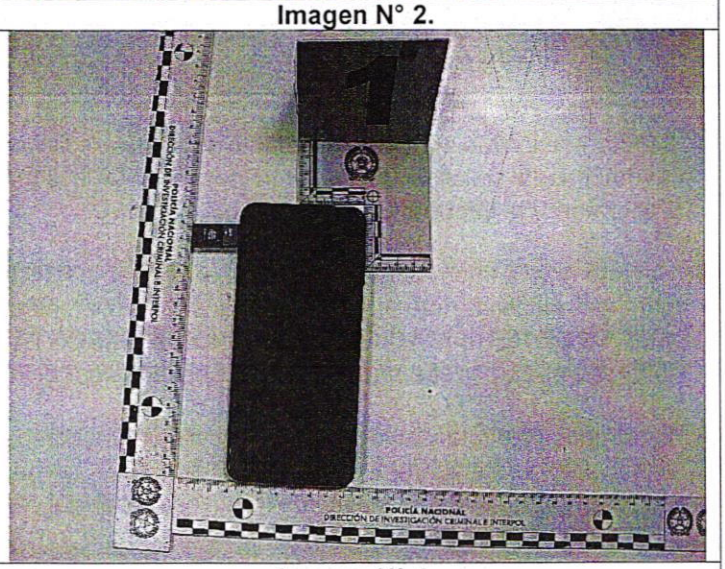

Imagen N° 4.

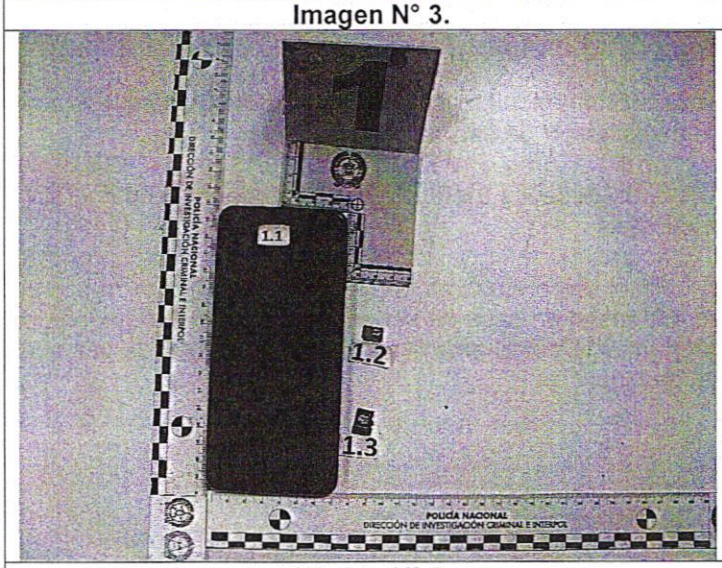

Imagen N° 5.

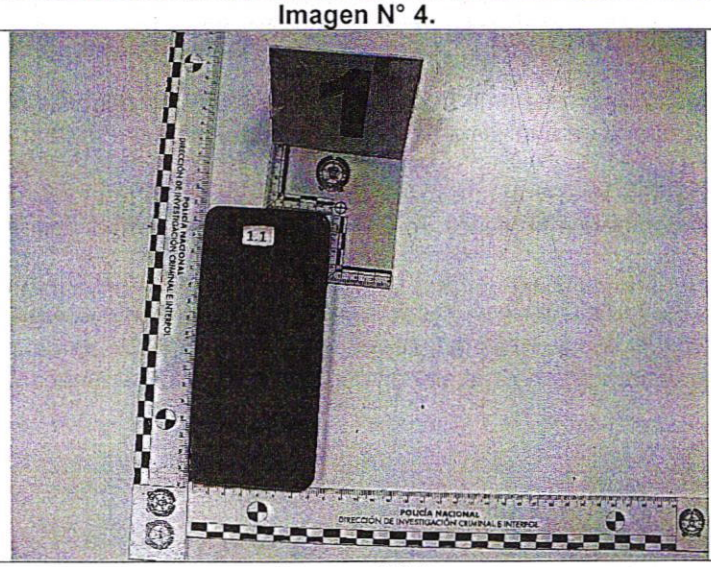

Imagen N° 6.

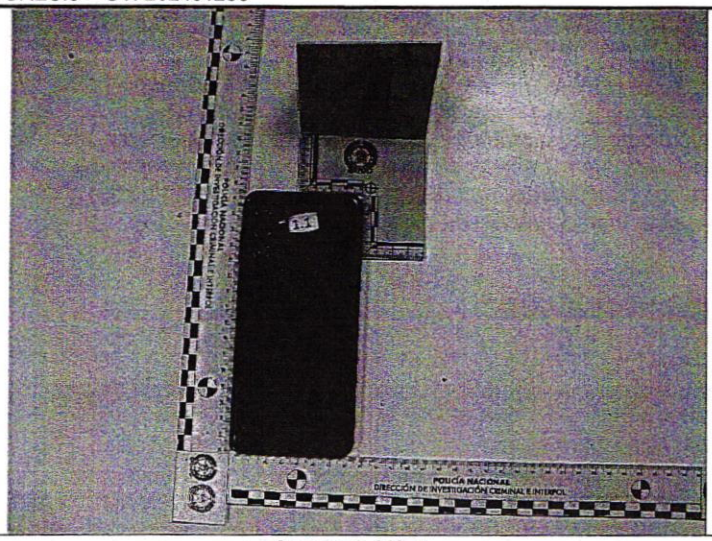

Imagen N° 7.

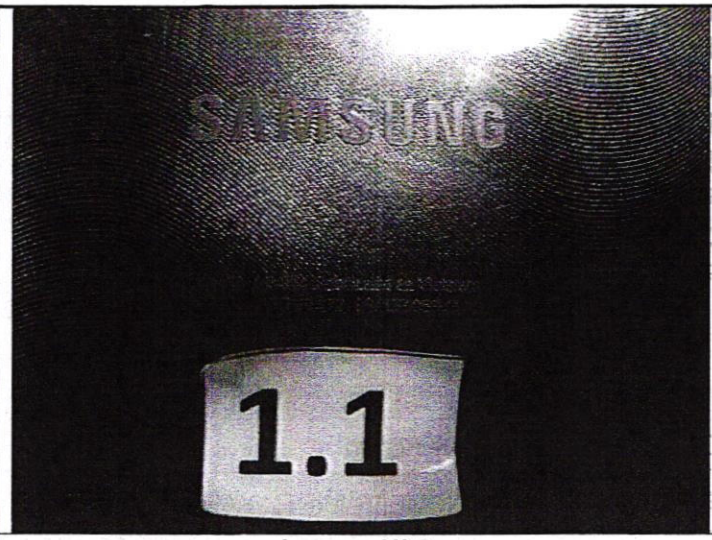

Imagen N° 8.

Imagen N° 9.

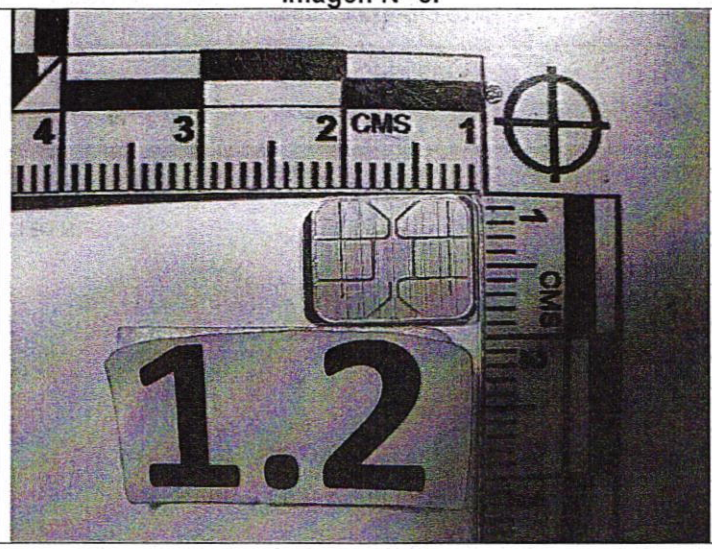

Imagen N° 10.

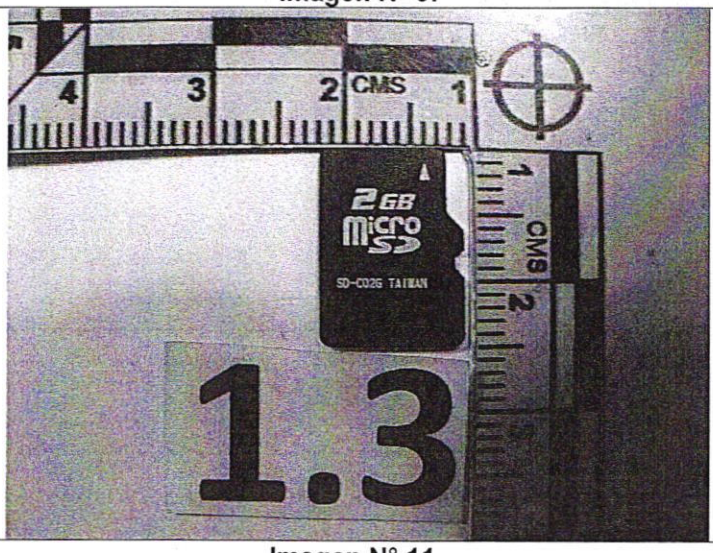

Imagen N° 11.

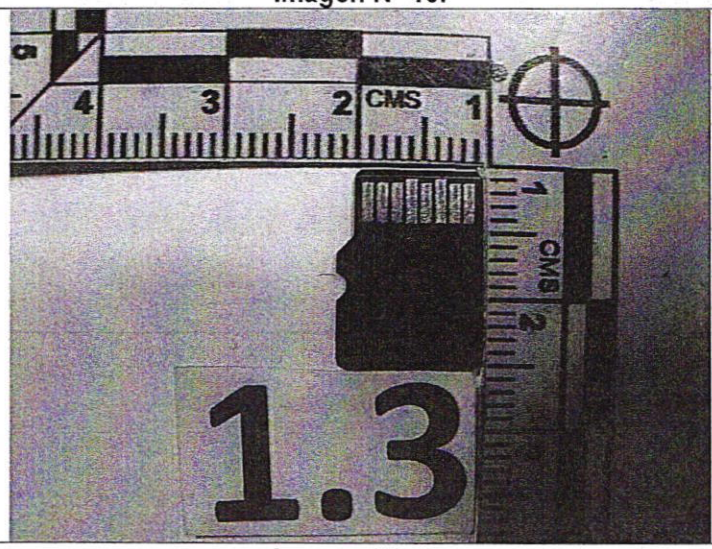

Imagen N° 12.

"De igual manera se trasfiere la reserva legal de la información, teniendo en cuenta que es responsabilidad del funcionario solicitante garantizar, que la información que origina o procesa la Dirección de Investigación Criminal e INTERPOL, debe mantener el principio de segmentación a partir de la necesidad de saber y conocer estrictamente lo necesario para el desempeño de la función que le es propia, el acceso, uso y disposición final de la misma, lo anterior teniendo en cuenta los parámetros establecidos en la ley 1581/2012 y la ley 1712/2014 que refiere a garantizar los derechos fundamentales, constitucionales y legales de los datos, enmarcadas en las actividades que realizan los funcionarios adscritos a la DIJIN en liderar la Investigación Criminal y apoyar la administración de Justicia".

INFORMACIÓN PÚBLICA RESERVADA

12. PERITO / SERVIDOR DE POLICÍA JUDICIAL

Nombres y Apellidos		Identificación	Entidad
SI. GERARDO ENRIQUE RAMIREZ YARA		80808872	POLICÍA NACIONAL
Cargo	Teléfono / Celular	Correo electrónico	Firma
PERITO	3223089274	Gerardo.ramirez1066@correo.policia.gov.co	

El servidor de policía judicial está obligado en todo tiempo a garantizar la reserva de la información, esto conforme a las disposiciones establecidas en la Constitución y la Ley.

FIN DEL INFORME