



# **UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA**

**FACULTAD DE INGENIERÍA EN SISTEMAS DE  
INFORMACIÓN**

**MAGISTER ARTIUM EN SEGURIDAD INFORMATICA**

## **PRÁCTICA NUMERO 4 DB**

**Autor (es):**

**Ventura Santa Cruz Marco Polo – mventuras@miumg.edu.gt**

**Ramos Figueroa Mavelin Estefani - mramosf2@miumg.edu.gt**

**Javier Fernando Camey Valenzuela – jcameyv1@miumg.edu.gt**

**Guerra Osorio Mario José – mguerra01@miumg.edu.gt**

**Profesor**

**Ing. Willy Peitzner Rosal**

**Curso**

**Metodologías para el análisis informático forense**

**7mo trimestre 2025**

**Guatemala, 2025**

## **Introducción**

La presente práctica de análisis forense de bases de datos y entornos en la nube representó un desafío significativo en la aplicación de técnicas de investigación digital avanzadas. El reto principal consistió en utilizar herramientas especializadas para analizar diferentes tipos de bases de datos, desde SQLite en dispositivos móviles hasta servidores MySQL, demostrando cómo la inteligencia forense se aplica en entornos diversos.

El análisis se abordó metódicamente en dos ejercicios principales: en primer lugar, se utilizó DB Browser for SQLite para investigar bases de datos de dispositivos Android, identificando información de cuentas y marcadores sincronizados. En segundo lugar, se empleó Hex Workshop para realizar análisis hexadecimal de archivos de base de datos MySQL, descubriendo actividades maliciosas como la creación de usuarios no autorizados y modificaciones a contenidos.

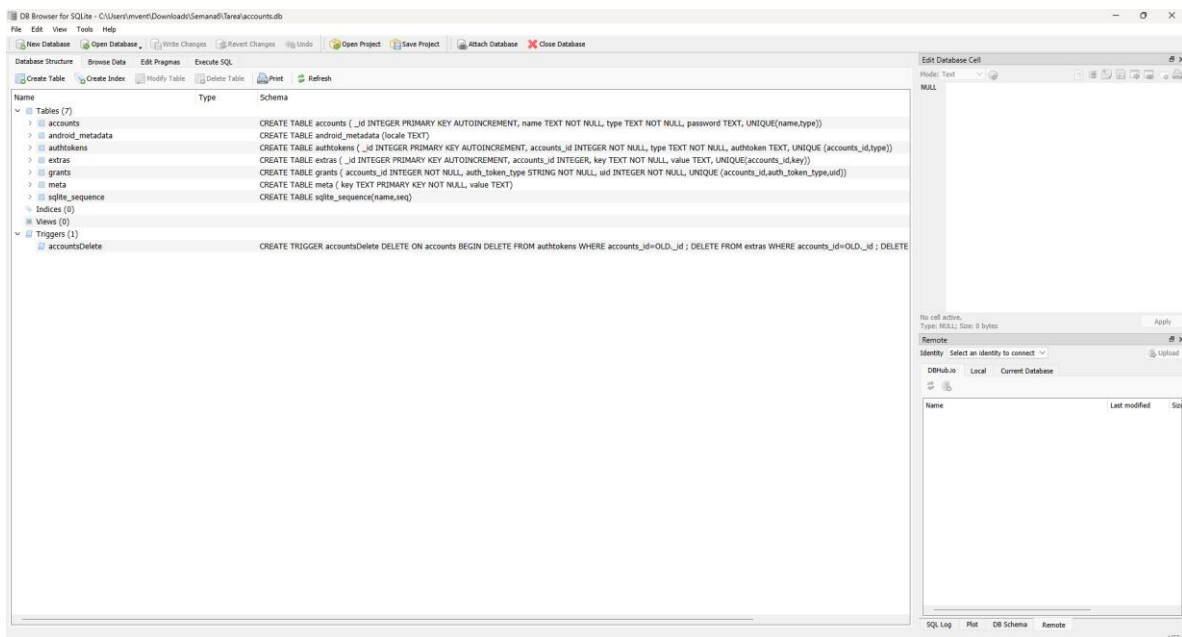
Ambos ejercicios demandaron la aplicación rigurosa de técnicas forenses específicas, desde la navegación estructurada en esquemas de bases de datos hasta el análisis de valores hexadecimales, enfrentando dificultades como la interpretación de datos fragmentados, la ausencia de documentación técnica y la necesidad de correlacionar información entre múltiples fuentes. A pesar de estos desafíos, se logró demostrar cómo la inteligencia forense puede adaptarse eficazmente a entornos diversos, garantizando la integridad y utilidad de los hallazgos obtenidos.

## Contenido

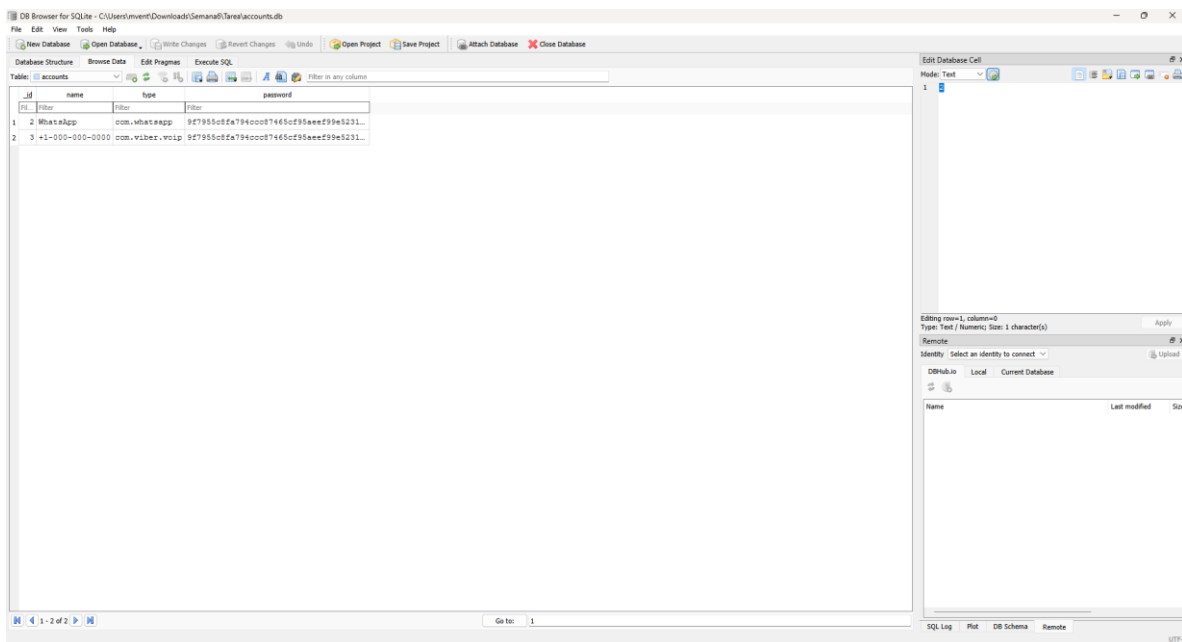
### Ejercicio 01 – Analizando bases de datos SQLite de dispositivo Android

#### Análisis del Archivo "accounts.db" con DB Browser for SQLite

Al abrir la base de datos "accounts.db" en DB Browser for SQLite, se procedió a examinar la estructura y contenido de las tablas existentes. Mediante la pestaña "Browse Data", se revisaron las tablas para identificar información relevante sobre cuentas sincronizadas en el dispositivo.



La imagen muestra DB Browser for SQLite con la base de datos accounts.db abierta, donde se listan varias tablas como accounts, authtokens, meta, extra y android\_metadata. Cada tabla incluye su sentencia CREATE TABLE, con campos clave como id, name, type, password y authtoken. También se observa un trigger llamado accountDbdelete, diseñado para eliminar registros de accounts y extra cuando ocurre una eliminación específica. Esta vista permite analizar la estructura interna de la base de datos, las relaciones entre tablas y la lógica definida para la gestión de datos.



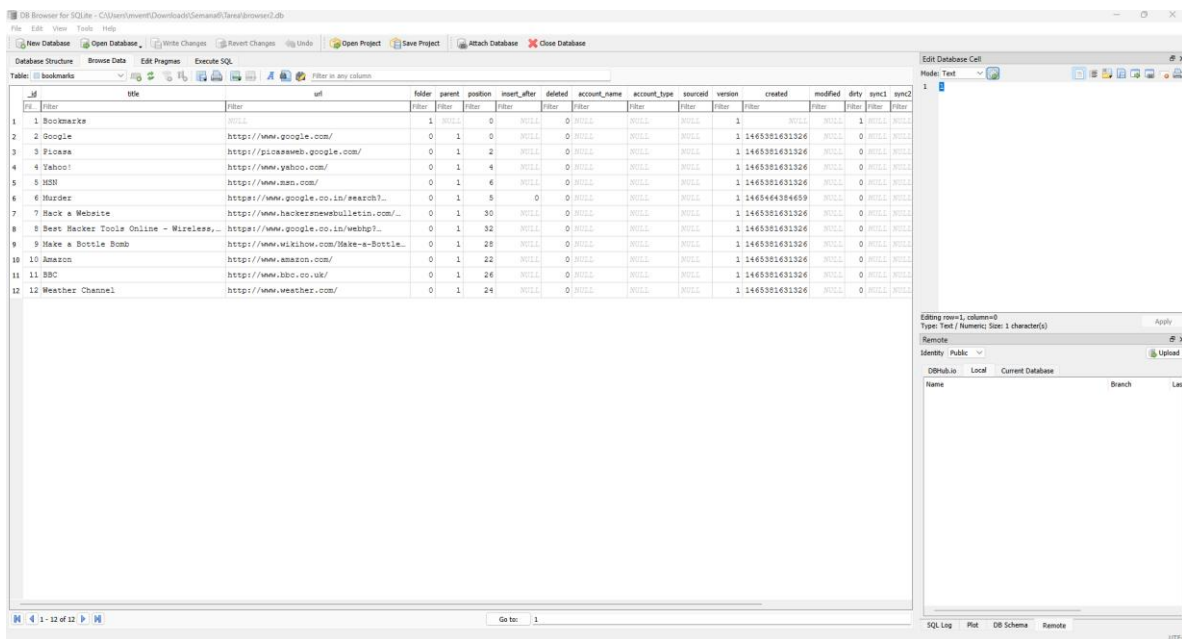
La imagen muestra DB Browser for SQLite con la base de datos accounts.db abierta en la pestaña Browse Data, donde se visualizan registros de la tabla accounts. Se observan campos como id, name, type y password, con ejemplos que incluyen cuentas de WhatsApp y Viber junto a sus tokens o credenciales cifradas. Esta vista es clave para extraer información de cuentas almacenadas en dispositivos y analizar datos sensibles durante una investigación forense o de seguridad.

### Procedimiento aplicado:

- Apertura de la base de datos SQLite con DB Browser
- Navegación through las diferentes tablas disponibles
- Análisis de los registros en la pestaña "Browse Data"

**Hallazgo concluyente:** El dispositivo estaba sincronizado con dos servicios de mensajería: WhatsApp y Viber. Esta información es crucial para entender el alcance de la recolección de datos y posibles vectores de exfiltración de información.

## Análisis del Archivo "browser2.db" con DB Browser for SQLite

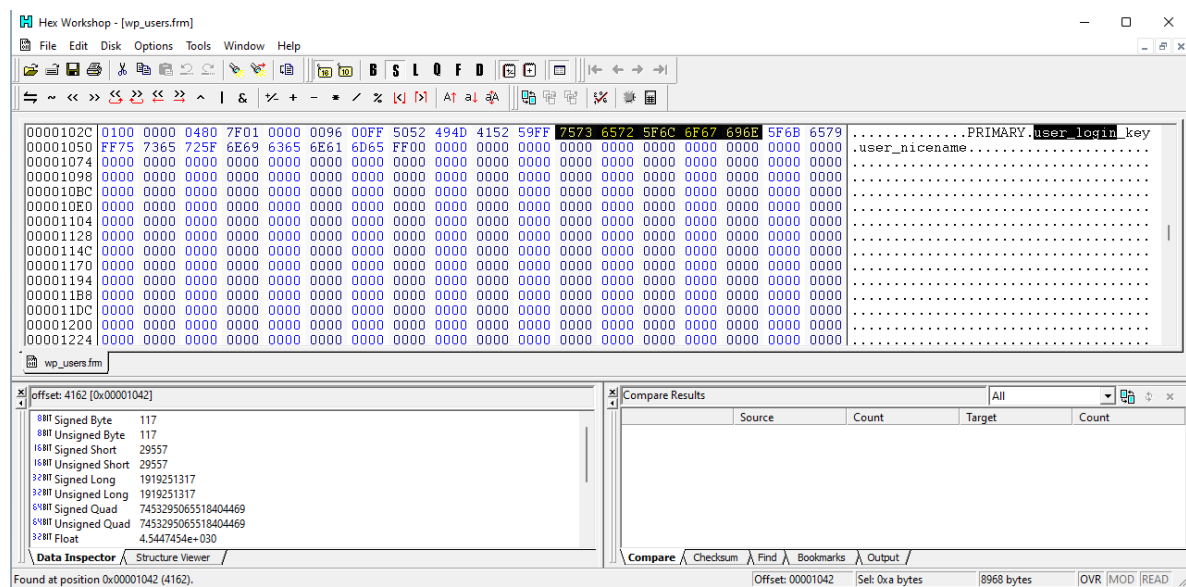


id	title	url	folder	parent	position	insert_after	deleted	account_name	account_type	sourceid	version	created	modified	dirty	sync1	sync2
1	Bookmarks		NULL	0	0	0	0	NULL	NULL	1	1	1465351631326	1465351631326	0	1	1465351631326
2	Google	http://www.google.com/	0	1	0	0	0	NULL	NULL	1	1	1465351631326	1465351631326	0	1	1465351631326
3	Picasa	http://picasaweb.google.com/	0	1	2	0	0	NULL	NULL	1	1	1465351631326	1465351631326	0	1	1465351631326
4	Yahoo!	http://www.yahoo.com/	0	1	4	0	0	NULL	NULL	1	1	1465351631326	1465351631326	0	1	1465351631326
5	MSN	http://www.msn.com/	0	1	6	0	0	NULL	NULL	1	1	1465351631326	1465351631326	0	1	1465351631326
6	Hacer	http://www.google.co.in/search?	0	1	5	0	0	NULL	NULL	1	1	1465464364659	1465464364659	0	1	1465464364659
7	Hack a Website	http://www.hacknewsbulletin.com/...	0	1	30	0	0	NULL	NULL	1	1	1465351631326	1465351631326	0	1	1465351631326
8	Beat Hacker Tools Online - Wireless...	http://www.google.co.in/webhp?...	0	1	32	0	0	NULL	NULL	1	1	1465351631326	1465351631326	0	1	1465351631326
9	Make a Bottle Bomb	http://www.wikihow.com/Make-a-Bottle...	0	1	28	0	0	NULL	NULL	1	1	1465351631326	1465351631326	0	1	1465351631326
10	Amazon	http://www.amazon.com/	0	1	22	0	0	NULL	NULL	1	1	1465351631326	1465351631326	0	1	1465351631326
11	BBC	http://www.bbc.co.uk/	0	1	26	0	0	NULL	NULL	1	1	1465351631326	1465351631326	0	1	1465351631326
12	Weather Channel	http://www.weather.com/	0	1	24	0	0	NULL	NULL	1	1	1465351631326	1465351631326	0	1	1465351631326

La imagen muestra DB Browser for SQLite con la base de datos browser2.db abierta en la pestaña Browse Data, visualizando el contenido de la tabla bookmarks. Se listan varios sitios web como Google, Yahoo, Facebook y Weather Channel con detalles como la URL, posición en la lista, fecha de creación, fecha de modificación y cuenta asociada. Esta vista es útil para analizar el historial o los marcadores de un usuario, permitiendo revisar patrones de navegación, intereses y posibles evidencias relevantes en un contexto de investigación forense.

**Hallazgo concluyente:** Los marcadores encontrados proporcionan información valiosa sobre el comportamiento de navegación del usuario, incluyendo posibles accesos a servicios en la nube, redes sociales, y otros recursos en línea.

## Ejercicio 02 – Análisis Forense de Base de Datos MYSQL Server



### Análisis del Archivo "wp\_users.frm" con Hex Workshop

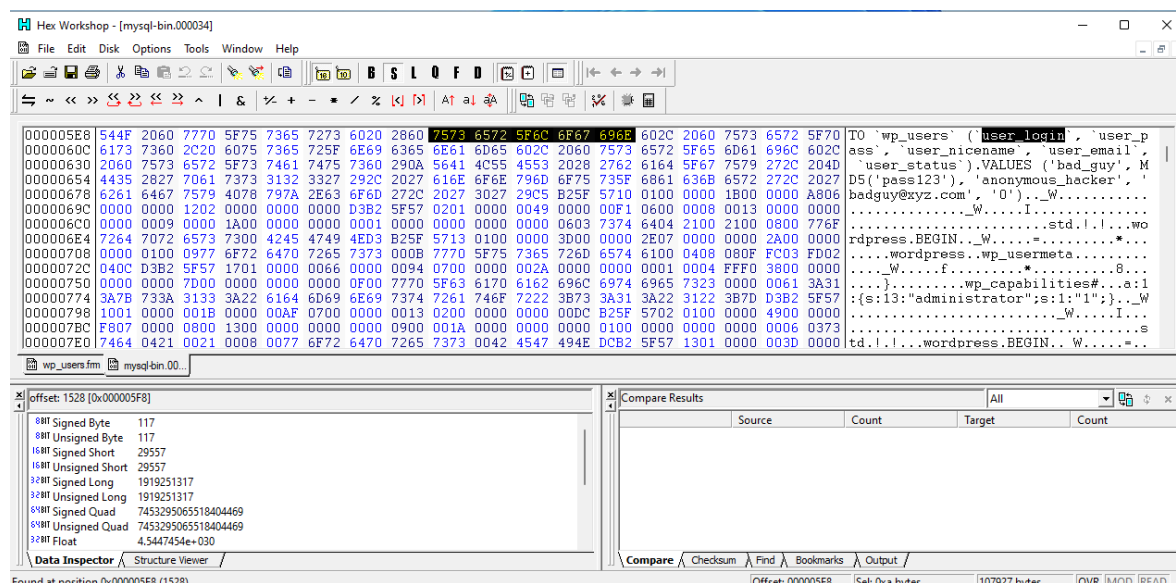
Se utilizó Hex Workshop para analizar el archivo "wp\_users.frm" en formato hexadecimal. Se buscó específicamente el valor hexadecimal 757365725F6C6F67696E que corresponde a "user\_login" en ASCII.

### Procedimiento aplicado:

- Apertura del archivo .frm en Hex Workshop
- Búsqueda del valor hexadecimal 757365725F6C6F67696E
- Identificación de nombres de usuario en la estructura de datos

**Hallazgo concluyente:** Se identificó el nombre de usuario "bad\_guy" utilizado por el atacante, confirmando la existencia de una cuenta no autorizada en el sistema WordPress.

## Análisis del Archivo "mysql-bin.000034" con Hex Workshop



Se examinó el archivo binario de log de MySQL para identificar queries ejecutados por el atacante. Se buscaron los mismos valores hexadecimales asociados a la creación de usuarios maliciosos.

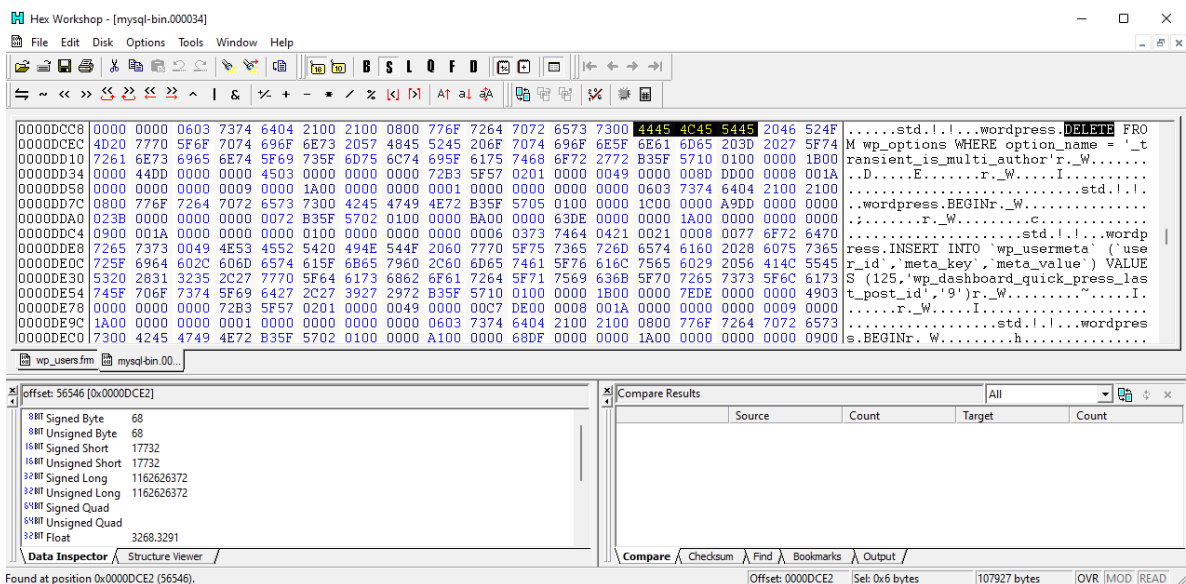
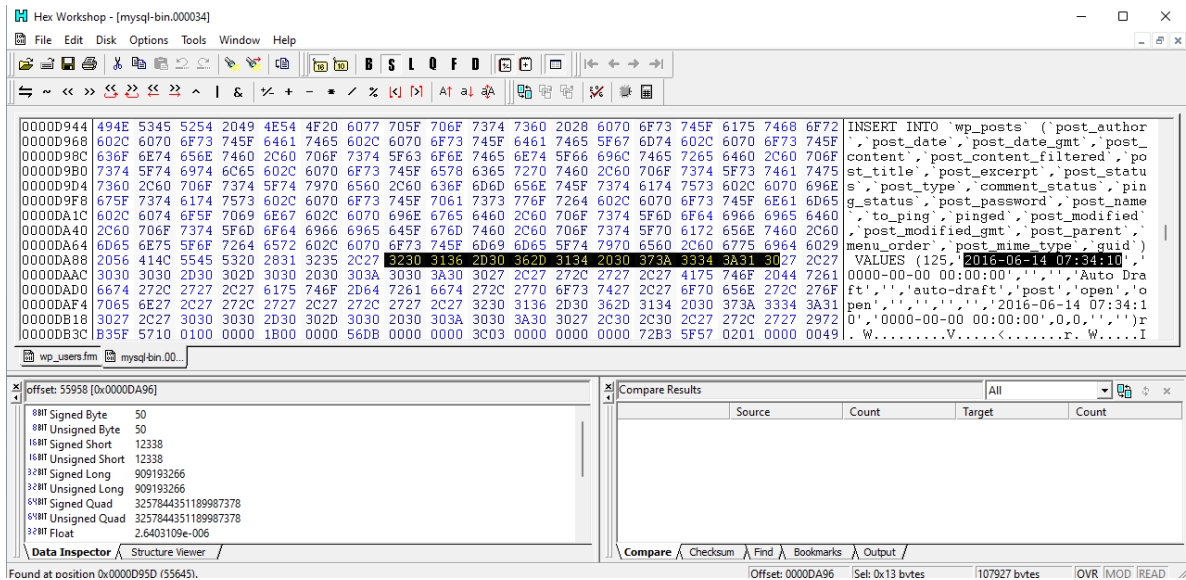
### Procedimiento aplicado:

- Búsqueda de queries de creación de usuario (CREATE USER)
- Identificación de valores hexadecimales correspondientes a credenciales
- Análisis de la estructura del query malicioso

**Hallazgo concluyente:** Se descubrió el query ejecutado para crear un usuario no autorizado con los siguientes datos:

- **Login name:** bad\_guy
- **Password:** pass123
- **Nice name:** anonymous\_hacker
- **Email ID:** [badguy@xyz.com](mailto:badguy@xyz.com)

### Análisis de Timestamps y Actividad Maliciosa



Mediante búsquedas adicionales con CTRL+F en Hex Workshop, se identificaron más actividades maliciosas:

## Hallazgos adicionales:

- **Post\_author id 125:** Se identificó una modificación de contenido realizada el **14 de junio de 2016 GMT 07:37:45**



- **Eliminación de usuarios:** Se encontraron queries de eliminación de usuarios legítimos
- **Modificación de posts:** Se detectaron alteraciones en contenidos del WordPress

### **Verificación de integridad de evidencias**

Se verificaron los hashes del archivo Evidencias.iso para garantizar la integridad forense:

- **MD5:** 3bde0591d2831896a8585ec0fa85f74b ✓
- **SHA1:** 301865dc9e9015ec092c5bd781ff2e9b700b7d67 ✓

La coincidencia de hashes confirmó que la evidencia no fue alterada durante el proceso de análisis.

## **Conclusiones**

### **Sobre Herramientas Utilizadas**

**DB Browser for SQLite** demostró ser una herramienta esencial para el análisis forense de bases de datos móviles. Su interfaz intuitiva permite navegar through tablas y registros eficientemente, mientras que su capacidad para ejecutar queries personalizados facilita búsquedas específicas. La herramienta resultó invaluable para analizar estructuras de datos en dispositAndroid.

**Hex Workshop** confirmó su utilidad en el análisis forense de bajo nivel. Su capacidad para trabajar con valores hexadecimales y realizar búsquedas avanzadas permitió descubrir información oculta en archivos de base de datos binarios. La funcionalidad de búsqueda de patrones hexadecimales resultó particularly útil para identificar strings específicos en grandes volúmenes de datos.

## **Hallazgos y Capacidades de Análisis**

El análisis reveló múltiples vectores de compromiso en bases de datos: desde la sincronización de cuentas en dispositivos móviles hasta la creación de usuarios maliciosos en servidores MySQL. Se demostró la importancia de:

- Analizar logs binarios de bases de datos para detectar actividades no autorizadas
- Verificar la integridad de estructuras de datos en aplicaciones web
- Monitorizar queries de administración de usuarios en sistemas críticos

## **Manejo de Evidencia y Criterio Experto**

El proceso destacó la critical importancia del análisis hexadecimal para investigaciones forenses avanzadas. La capacidad de interpretar valores hex y correlacionarlos con actividades maliciosas demostró un criterio experto en la investigación digital. El uso de técnicas de búsqueda pattern-based en grandes archivos binarios mostró un enfoque metodológico sólido.

## **Recomendaciones de Seguridad**

1. **Monitorizar queries de administración** en bases de datos críticas
2. **Implementar logging extensivo** de todas las operaciones de base de datos
3. **Revisar regularmente** usuarios y permisos en sistemas WordPress
4. **Auditar sincronizaciones** de cuentas en dispositivos móviles
5. **Capacitar administradores** en detección de actividades sospechosas en bases de datos

23:18  
20/08/2023

ESP

MARCO POLO VENTURA SANTA CRUZ

JAVIER FERNANDO CAMEY VALENZUELA

MAVELIN ESTEFANI RAMOS FIGUEROA

MARIO JOSÉ

23:18 | cae-yiof-few