OWASP

Open Web Application Security Project

# Extracción lógica de dispositivos Android con Linux

# Gustavo A. Martin M.

- Licenciado en Computación.
- Experiencia en el área de informática forense y Seguridad Informática.
- Antiguo Miembro del Centro Nacional de Informática Forense (CENIF).


- Actualmente miembro del Sistema Nacional de Gestión de Incidentes Telemáticos (VenCERT).

VenCERT

OWASP
Open Web Application Security Project

# Agenda

- Lo bueno y lo malo
- Encontré un Android ¿Qué hago?
- ¿Cómo demuestro lo que hago?
- Ejercitemos un poco
- Conclusiones

# Extracción de dispositivos Android

## Lo Bueno

- Es posible obtener información valiosa para una investigación.


**Un celular decomisado, clave en la captura de 'El Chapo'**

http://www.forbes.com.mx/un-celular-decomisado-clave-en-la-captura-de-el-chapo/

# Extracción de dispositivos Android

## Lo Bueno

- Permite agilizar el trabajo de recopilación de información en un crimen.

- No daña el dispositivo.

# Extracción de dispositivos Android

## Lo Malo

- La información recolectada debe cumplir con procedimientos adecuados.
- Se puede encontrar información sensible la cual debe ser tratada con la debida cautela y discreción.

# Encontré un Android ¿Qué hago?

- Doctrina del fruto del árbol envenenado.
- Principio de Locard.
- NIST 800-88r1, para el purgado del disco copia donde se analizará la evidencia.
- RFC 3227, Guía para recolectar y archivar evidencias.
- ISO 27037, Directrices para la identificación, recolección, consolidación y preservación de evidencia digital.

# Encontré un Android ¿Qué hago?

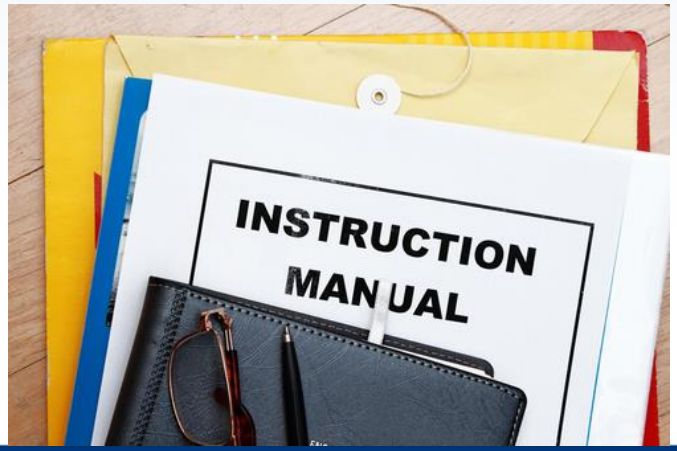
- Siempre trabajar con inhibidores de señal o en su defecto bolsas Faraday.
- Mantener una cadena de custodia del dispositivo desde el momento de la recolección hasta la entrega.

# Bolsas Faraday e inhibidores de señal


OWASP
Open Web Application Security Project

# ¿Cómo demuestro lo que hago?

- Debe contarse con manuales de procedimiento.
- Basarse por metodologías para tratar con la evidencia.




# ¿Cómo demuestro lo que hago?

Un buen informe permitirá a cualquier perito validar tus resultados y evitará preguntas de los jueces en un juicio.

# Ejercitemos un poco

Realizaremos una extracción lógica a un dispositivo android para encontrar:

- Registro de llamadas
- Registro de mensajes SMS
- Registro de mensajes MMS
- Contactos

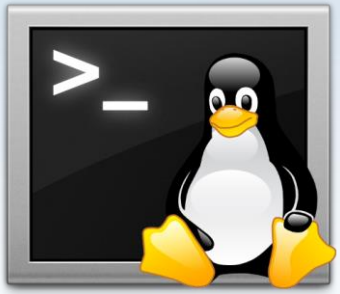
OWASP
Open Web Application Security Project

# Ejercitemos un poco

¿Que usaremos?

- Santoku Linux


- Terminal de Linux



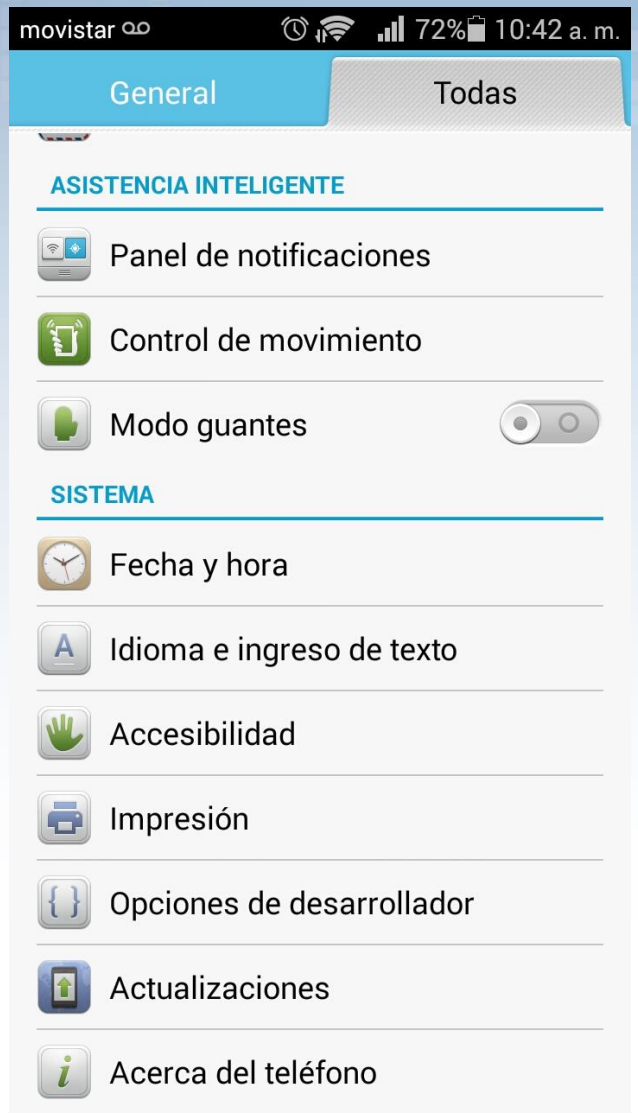
- AFLogical OSE

- Dispositivo en modo depuración y permitiendo instalación de orígenes desconocidos.

# Ejercitemos un poco

Modo Depuración en dispositivos Android

# Ejercitemos un poco




Para versiones de Android hasta la 3.x se va de esta manera Ajustes -> Aplicaciones -> Desarrollo, a continuación, "Depuración USB".

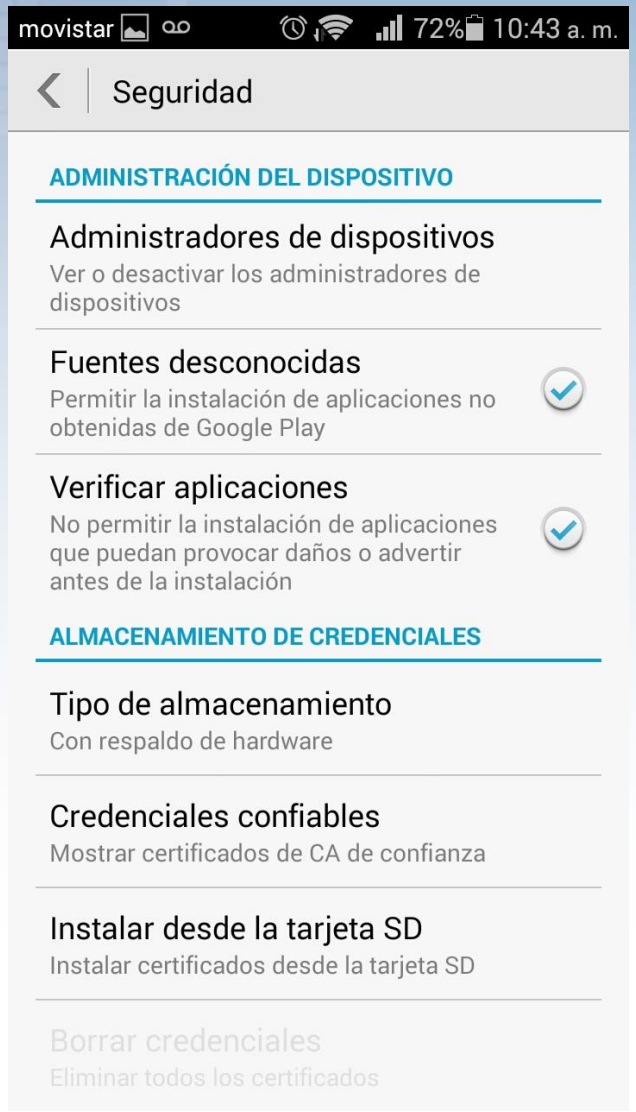
En Android 4.x y superiores se encuentra en Configuración -> Opciones de Desarrollador, por ultimo "Depuración USB".

OWASP
Open Web Application Security Project

# Ejercitemos un poco

Permitir Orígenes Desconocidos

# Ejercitemos un poco




Se encuentra en Ajustes -> Seguridad -> “Fuentes desconocidas”.

OWASP
Open Web Application Security Project

# Conclusiones

- Con la extracción lógica podemos obtener información que se encuentra en el dispositivo.
- Este no es el único método de extracción que existe para dispositivos Android.
- La información que se borra del dispositivo no puede ser recuperada bajo este método.

# Gracias.

@gustavoadolfomm