

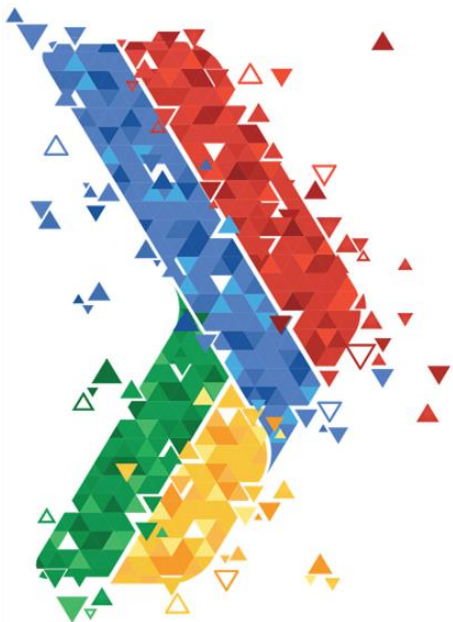
# “Peritaje informático: Investigación forense en dispositivos Android”

Por: Clara Flores Siñani



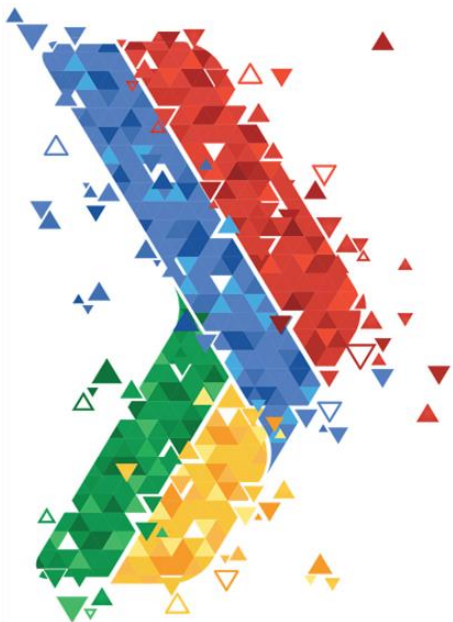
# Pruebas digitales en dispositivos móviles (1/2)

- historial de llamadas,
- mensajes de texto,
- correos electrónicos,
- fotografías digitales,
- videos,
- entradas de calendario,
- notas,
- agenda con nombres, teléfonos, empresas y direcciones de contacto,
- contraseñas o
- números de tarjetas de crédito.



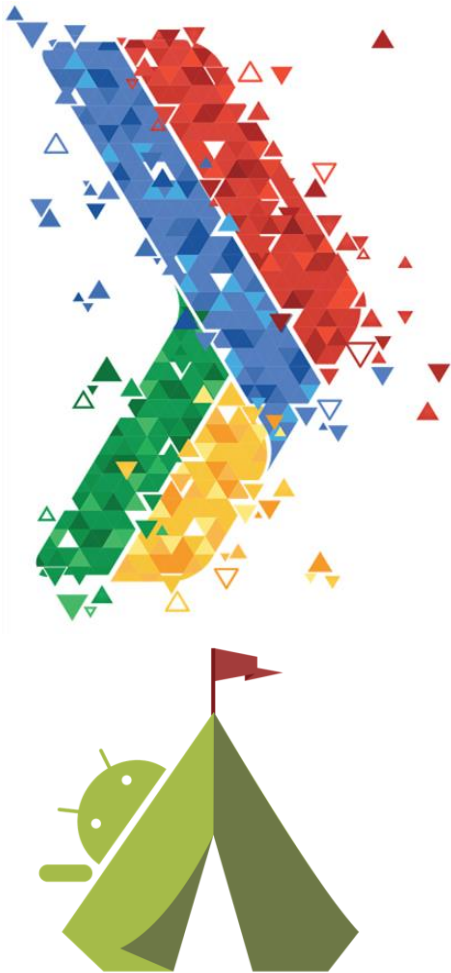
# Pruebas digitales en dispositivos móviles (2/2)

- Además de utilizarse como terminal de telefonía,
- También se emplean para intercambiar fotografías, acceder a internet, conectarse a redes sociales, mantener blogs personales, tomar notas, grabar y consumir video y audio, etc.



# Información en los móviles

- metadatos de fecha, hora, latitud, longitud y altitud que pudieran contener las fotografías realizadas con el móvil, con los pequeños error de su GPS.
- mediante la secuencia de antenas móviles a las que se ha ido conectando, si bien, con una mayor imprecisión, pudiendo establecerse zonas más que posiciones concretas.





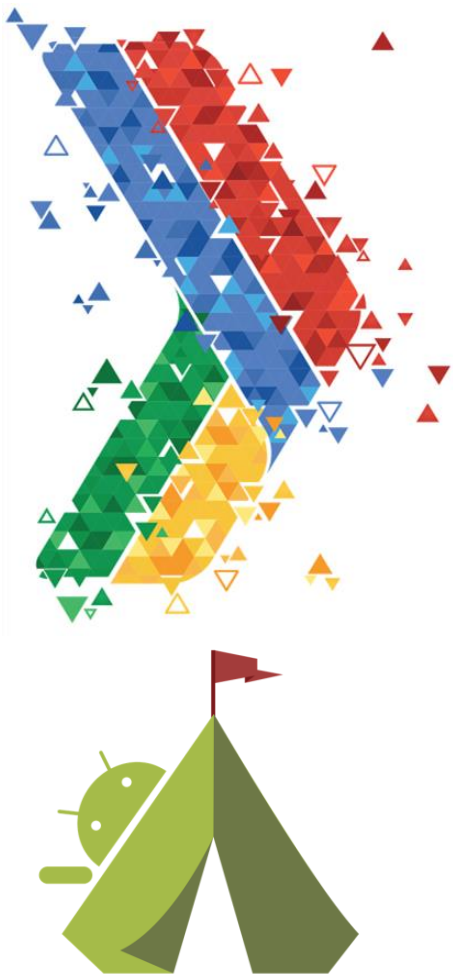
# Conceptos Clave



# Informática Forense

La informática forense a nivel mundial es la ciencia dedicada a la **recolección**, **preservación**, **análisis** y **presentación** de la evidencia digital en casos judiciales, arbitrales o procesos internos disciplinarios.

(\*) <http://confseguridad.upb.edu/programa/informatica-forense/>



# Cadena de Custodia

Procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis (peritos), con el fin de evitar alteraciones, sustituciones, contaminaciones o destrucciones.



# Evidencia Digital

Denominada también prueba electrónica es cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda puede ser utilizada en el juicio.



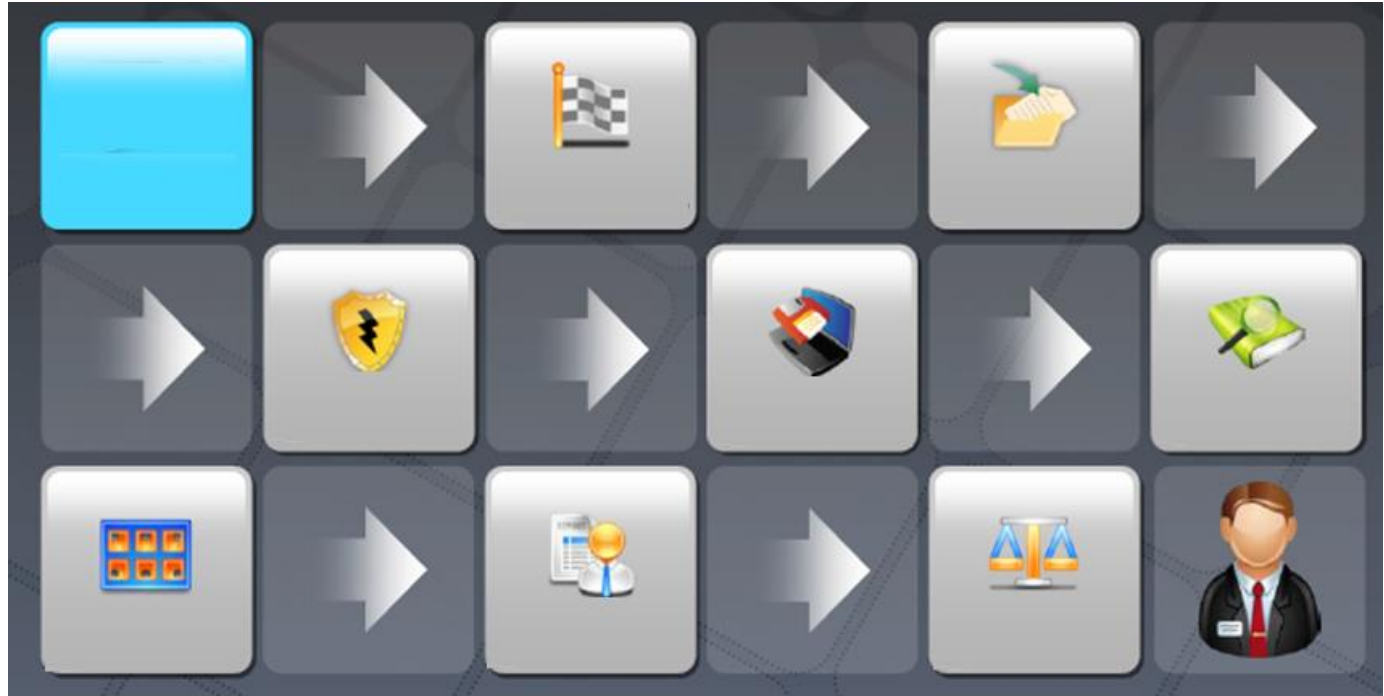
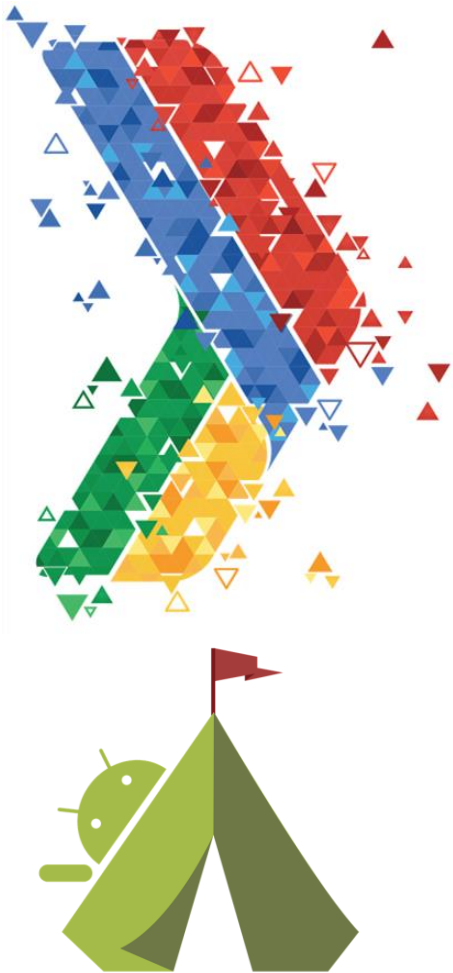




# Procedimiento



# METODOLOGIA DE LA INFORMATICA FORENSE



# EQUIPO DE INVESTIGACION FORENSE



Abogado



Fotógrafo



Alta Dirección  
o delegado



OSI



Examinador  
de la  
Evidencia

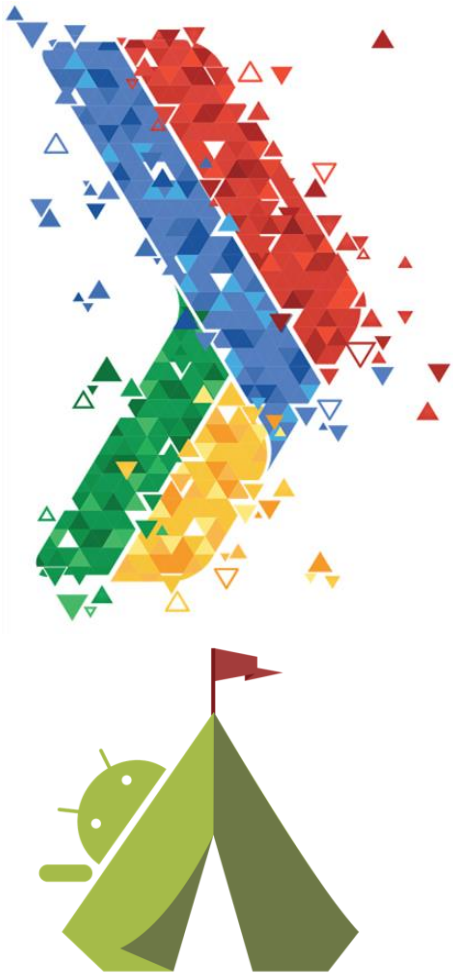


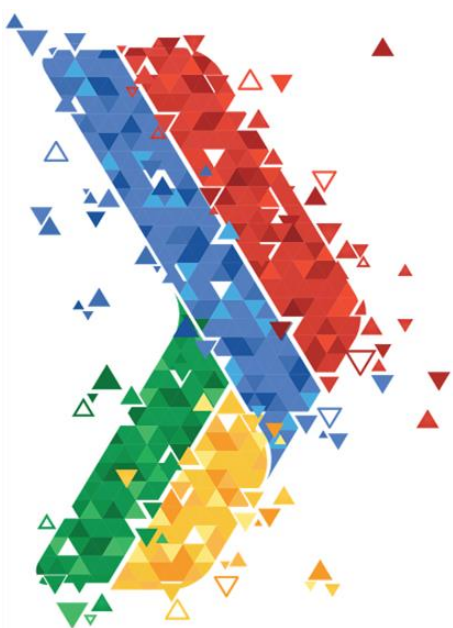
Documentador  
de la evidencia



# FORENSE ORIENTADO A MOVILES

En el desarrollo del proceso forense digital enfocado a teléfonos móviles se debe tener en cuenta la incautación, transportación y examinación segura.



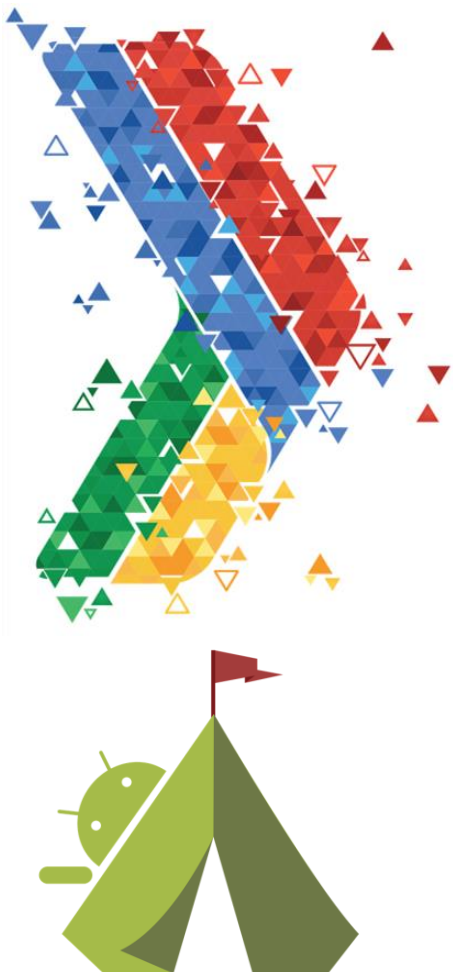


# Leyes que sustentan el Inicio del Proceso Forense

## ARTICULO 363 bis.- (MANIPULACIÓN INFORMÁTICA).-

*“El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días”*

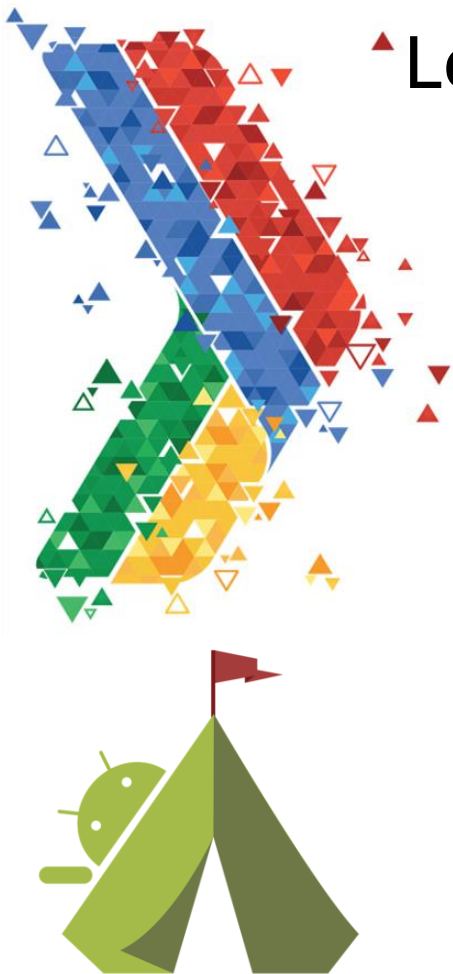
Capítulo XI del Código Penal Boliviano



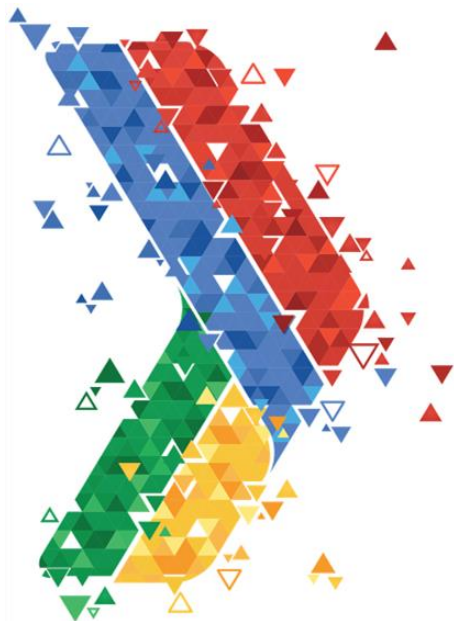
# ▲ Leyes que sustentan el Inicio del Proceso Forense

## **ARTICULO 363 Ter.- (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS).-**

*“El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días”.*





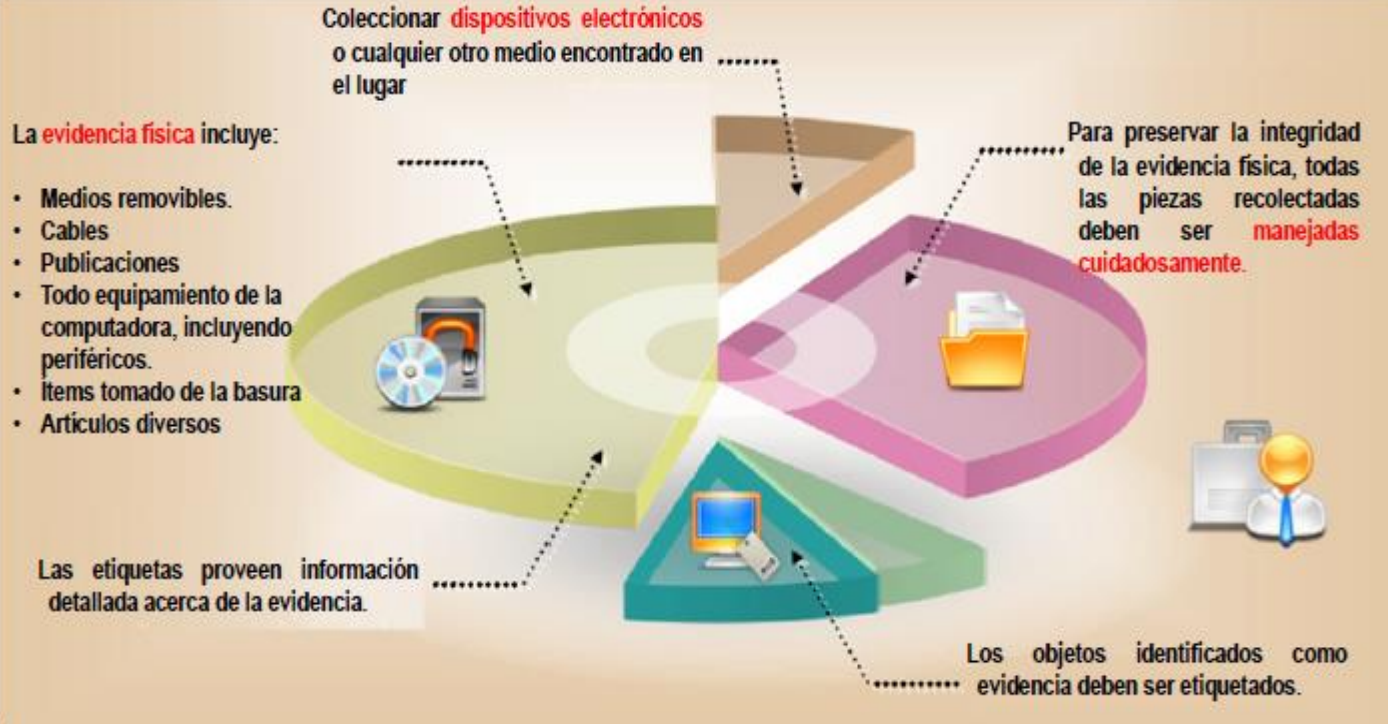


# Colección de evidencia





# RECOLECTAR EVIDENCIA FISICA



# RECOLECTAR EVIDENCIA LOGICA

**Lista de los sistemas** involucrados en el incidente y de la cual se puede obtener la evidencia.



Por cada sistema, obtener por **orden volatilidad** la evidencia relevante



registrar el grado de **sincronización del reloj del sistema.**



Recoger las pruebas de las **personas** que forman parte del incidente

Registrar el numero de serie electrónico del dispositivo

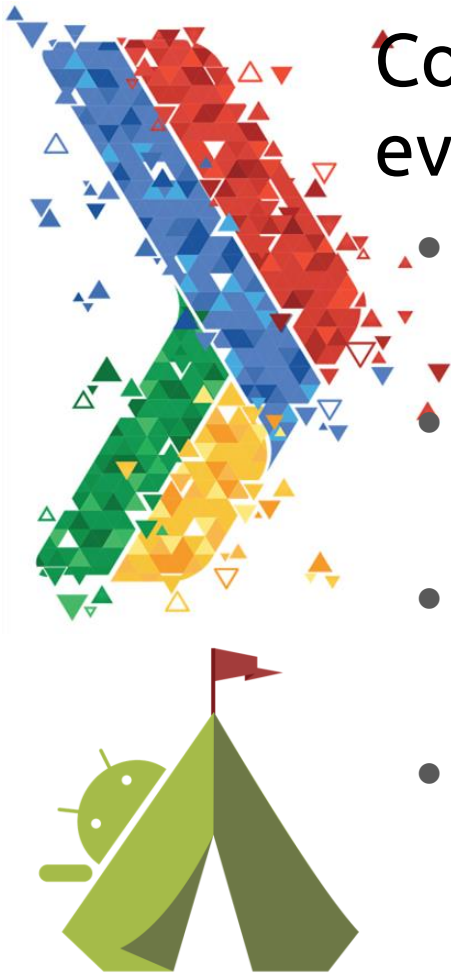



**Protección contra escritura y verificación de la presencia de virus** para mantener la integridad de los medios



# Consideraciones en la colección de evidencia Digital (1/2)

- El investigador forense digital es la persona idónea para considerar el equipo necesario para realizar la colección.
- Tener en cuenta la autoridad legal para realizar la recolección de pruebas.
- Solamente el personal a cargo debe estar presente en la recolección.
- Solicitar información al usuario del teléfono móvil para determinar el número de teléfono, códigos de acceso, patrones de bloqueo, PINs. (Aplica según la jurisdicción)






# Consideraciones en la colección de evidencia Digital (2/2)

- Si el teléfono móvil no puede ser analizado inmediatamente, **apagar el teléfono, retirar la batería** (si aplica) y **no encenderlo**
- Las ventajas de apagar el teléfono móvil son las siguientes:
  - Preservar los registros de llamadas y la última antena de telefonía móvil que brinda información de localización (LOCI).
  - La prevención de sobrescribir los datos eliminados.
  - La prevención de señales que intenten destruir datos del teléfono móvil.
  - Evitar la manipulación indebida.





# Consideraciones en la colección de evidencia Digital 3/3

Las desventajas o riesgos de apagar el teléfono móvil:

- Posibilidad de acoplamiento de mecanismos de autenticación (ejemplo, contraseñas, PINs, etc.) esto requiere que la recolección de información sea inmediata, por lo que necesita estar encendido pero aislado de cualquier red manteniendo al mismo tiempo la carga del teléfono.
- Blindaje contra la Radio Frecuencia (RF), esta comunicación podría alterar la información del teléfono móvil.
- Establecer el modo “avión” limitando el acceso a torres telefónicas, pero debe considerar las llamadas al 911.



# EL SISTEMA DE CLASIFICACIÓN DE HERRAMIENTAS FORENSES DE DISPOSITIVOS MÓVILES

Desarrollado por Sam Brothers, consiste en la *Pirámide Móvil Forense* Para la adquisición de datos y la clasificación de herramientas





## EL SISTEMA DE CLASIFICACIÓN DE HERRAMIENTAS FORENSES DE DISPOSITIVOS MÓVILES

**NIVEL 1** - El sistema de clasificación comienza en la parte inferior de la pirámide con la extracción manual.

**NIVEL 2** – la Extracción Lógica utiliza una variedad de protocolos para comunicarse con el sistema operativo del dispositivo a través de una serie de comandos.(Bluetooth o infrarrojos)

**NIVEL 3** – En la extracción física es donde comienzan las herramientas a permitir el acceso al espacio no asignado mediante el uso de conexiones JTAG y cajas de intermitencia.



## EL SISTEMA DE CLASIFICACIÓN DE HERRAMIENTAS FORENSES DE DISPOSITIVOS MÓVILES

**NIVEL 4** - El Chip-Off implica el removimiento tanto del chip NAND o NOR de un dispositivo móvil (volcado binario).

**Nivel 5** - El Micro Read es cuando el chip de seguridad ya se ha removido (o se encuentra severamente dañado) y sólo una porción del chip permanece.







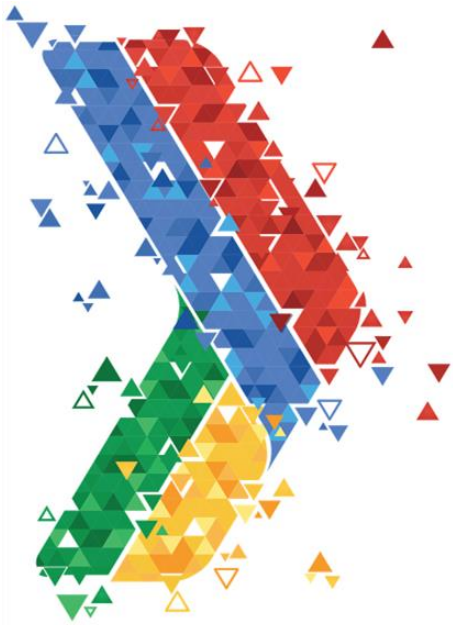
# Herramientas



# EJEMPLOS DE HERRAMIENTAS SEGÚN SU NIVEL

## Nivel 1:

- Ramsey's - STE3000FAV2 \$2,795.00
- Ramsey's - STE3000F2 \$ 1,695.00
- Ramsey's - STE3300F2 \$1,195.00
- Fernico's - ZRT 2 HD
- Fernico's – FAR



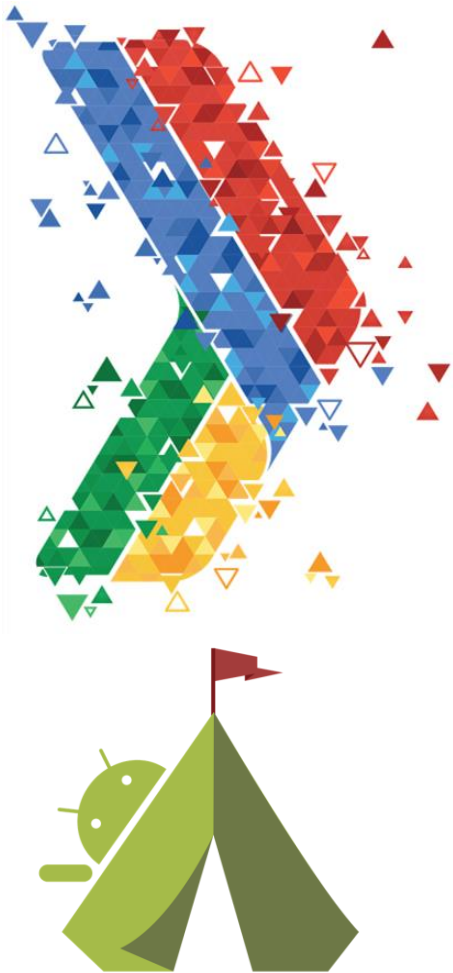
# EJEMPLOS DE HERRAMIENTAS SEGÚN SU NIVEL

## Nivel 2:

- Susteen's Secure View 3
- Compelson Labs's MOBILedit - Phone Forensics Express \$ 1,299.00

## Nivel 3:

- Micro Systemation's XRY
- Cellebrite's UFED Touch



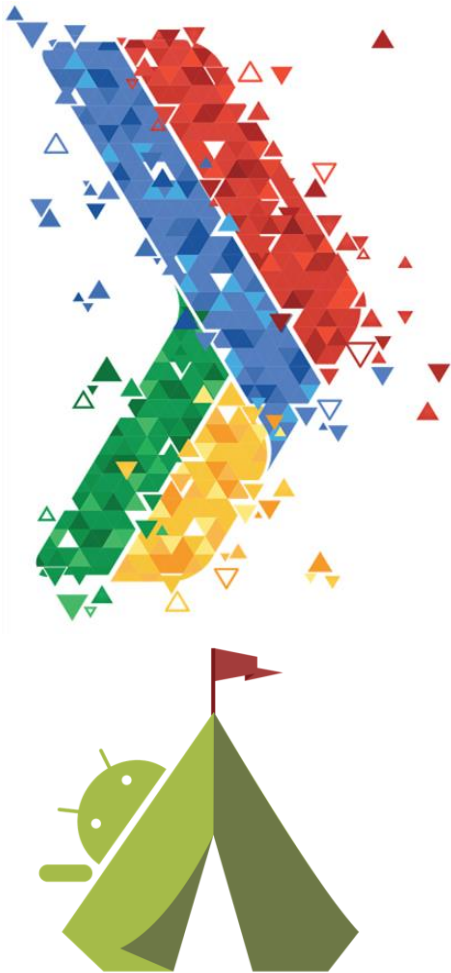
# EJEMPLOS DE HERRAMIENTAS SEGÚN SU NIVEL

## Nivel 4:

- Soft-Center's Flash Extractor - \$1,870.00
- JingTian SBGA128P memory ic Socket Adapter for up-828P up818P - \$415

## Nivel 5:

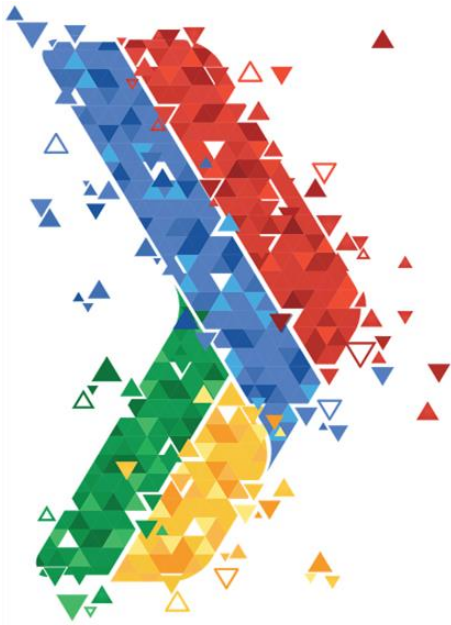
- Hitachi's S-450 SEM
- ERSA's IR 550



# Bolsas Faraday

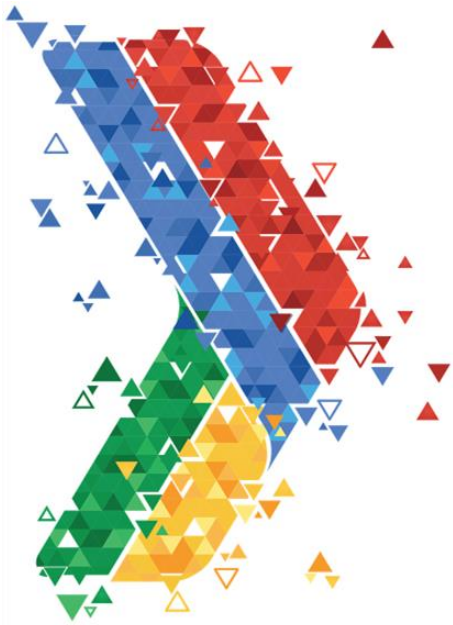
Recintos formados por mallas conductoras de varias capas, recubiertas por nylon ripstop y en el exterior cubiertas por poliuretano





- Evitan la conectividad a las redes celulares, WiFi y Bluetooth, esto por si de forma remota el sospechoso intenta borrar los datos.
- El blindaje eficaz a conexiones: 2G, 3G, 4G, LTE, Bluetooth (1, 2, 3 y 4), WiFi (2.4 GHz y 5 GHz), SatNav/GPS, RFID (HF), RFID (ACTIVE), RFID (UHF), entre otras.
- Dan garantía ya que son construidas bajo la normas ISO/IEC9001-2008.

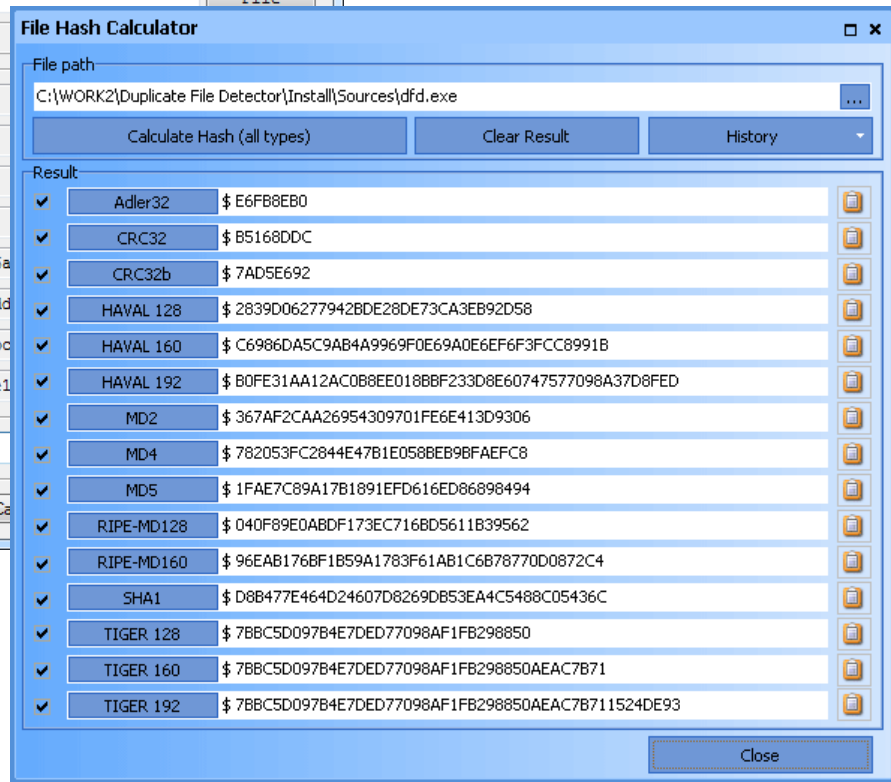
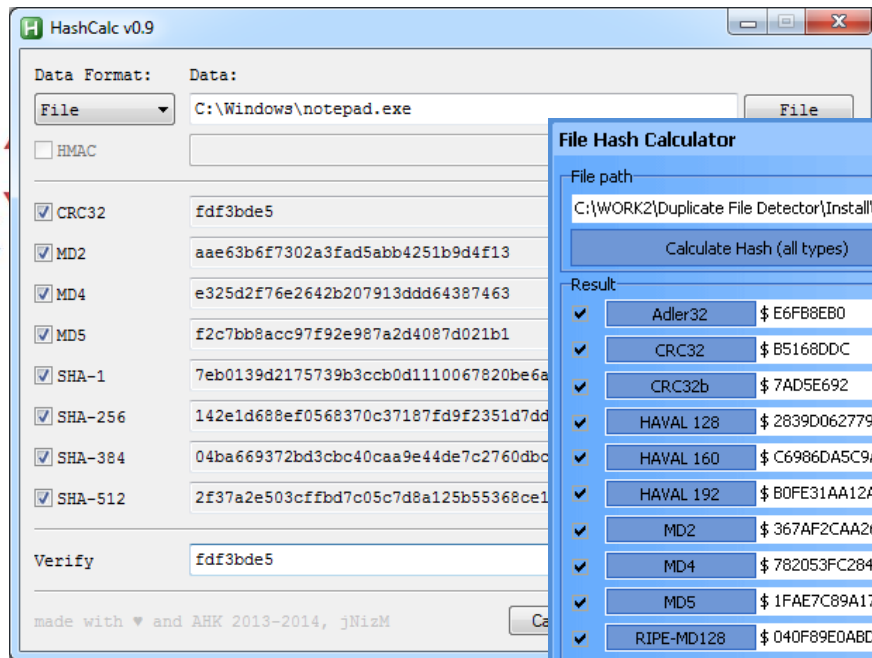




- Evitan el problema del bloqueo del PIN y PUK.
- Acelera los tiempos de investigación.
- Reduce costos
- Son reutilizables

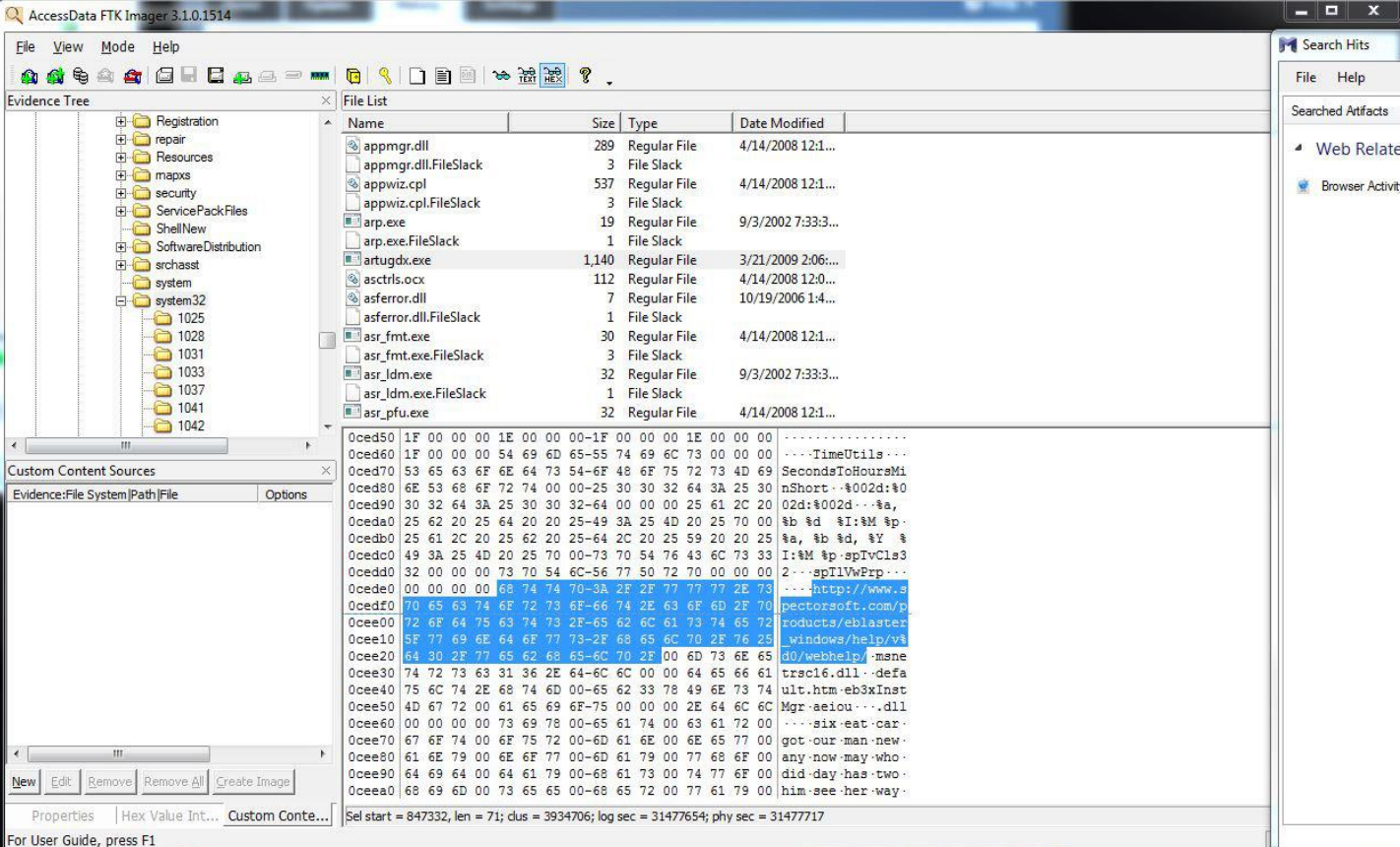


# VERIFICAR LA INTEGRIDAD DE DATOS





# FTK IMAGER



AccessData FTK Imager 3.1.0.1514

File View Mode Help

Evidence Tree

- Registration
- repair
- Resources
- mapxs
- security
- ServicePackFiles
- ShellNew
- SoftwareDistribution
- srchasst
- system
- system32
  - 1025
  - 1028
  - 1031
  - 1033
  - 1037
  - 1041
  - 1042

File List

Name	Size	Type	Date Modified
appmgr.dll	289	Regular File	4/14/2008 12:1...
appmgr.dll.FileSlack	3	File Slack	
appwiz.cpl	537	Regular File	4/14/2008 12:1...
appwiz.cpl.FileSlack	3	File Slack	
arp.exe	19	Regular File	9/3/2002 7:33:3...
arp.exe.FileSlack	1	File Slack	
artugdx.exe	1,140	Regular File	3/21/2009 2:06...
asctrls.ocx	112	Regular File	4/14/2008 12:0...
asferror.dll	7	Regular File	10/19/2006 1:4...
asferror.dll.FileSlack	1	File Slack	
asr_fmt.exe	30	Regular File	4/14/2008 12:1...
asr_fmt.exe.FileSlack	3	File Slack	
asr_idm.exe	32	Regular File	9/3/2002 7:33:3...
asr_idm.exe.FileSlack	1	File Slack	
asr_pfu.exe	32	Regular File	4/14/2008 12:1...

Custom Content Sources

Evidence:File System|Path|File Options

Hex View

```
0ced50 1F 00 00 00 1E 00 00 00 1F 00 00 00 1E 00 00 00 .....
0ced60 1F 00 00 00 54 69 6D 65-55 74 69 6C 73 00 00 00 ....TimeUtils...
0ced70 53 65 63 6F 6E 64 73 54-6F 48 6F 75 72 73 4D 69 SecondsToHoursMi
0ced80 6E 53 68 6F 72 74 00 00-25 30 30 32 64 3A 25 30 nShort..%002d:%0
0ced90 30 32 64 3A 25 30 30 32-64 00 00 00 25 61 2C 20 02d:%002d...%a,
0ceda0 25 62 20 25 64 20 20 25-49 3A 25 4D 20 25 70 00 %b %d %I:M %p-
0cedb0 25 61 2C 20 25 62 20 25-64 2C 20 25 59 20 20 25 %a, %b %d, %Y %
0cedc0 49 3A 25 4D 20 25 70 00-73 70 54 76 43 6C 73 33 I:%M %p-spIvCls3
0cedd0 32 00 00 00 73 70 54 6C-56 77 50 72 70 00 00 00 2...spIIVvFrp...
0cede0 00 00 00 00 68 74 74 70-3A 2F 77 77 77 7E 73 ....http://www.s
0cedf0 70 65 63 74 6F 72 73 6F-66 74 2E 63 6F 6D 2F 70 irectorsoft.com/p
0cee00 72 6F 64 75 63 74 73 2F-65 62 6C 61 73 74 65 72  roducts/ebblaster
0cee10 5F 77 69 6E 64 6E 77 73-2F 68 65 6C 70 2E 76 25 windows/help/va
0cee20 64 30 2F 77 65 62 68 65-6C 70 2F 00 6D 73 6E 65 d0/webhelp/.msne
0cee30 74 72 73 63 31 36 2E 64-6C 6C 00 64 65 66 61 trsc16.dll--defa
0cee40 75 6C 74 2E 68 74 6D 00-65 62 33 78 49 6E 73 74 ult.htm-eb3xInst
0cee50 4D 67 72 00 61 65 69 6F-75 00 00 00 2E 64 6C 6C Mgr-aeiou....dll
0cee60 00 00 00 00 73 69 78 00-65 61 74 00 63 61 72 00 ....six-eat-car-
0cee70 67 6F 74 00 6F 75 72 00-6D 61 6E 00 6E 65 77 00 got-our-man-new-
0cee80 61 6E 79 00 6E 6F 77 00-6D 61 79 00 77 68 6F 00 any-now-may-who-
0cee90 64 69 64 00 64 61 79 00-68 61 73 00 74 77 6F 00 did-day-has-two-
0ceea0 68 69 6D 00 73 65 65 00-68 65 72 00 77 61 79 00 him-see-her-way-
```

Search Hits

File Help

Searched Artifacts

Web Related

Browser Activity

Properties | Hex Value Int... Custom Conte...

For User Guide, press F1

# Andriller

Es una utilidad de software con una colección de herramientas forenses para teléfonos inteligentes.



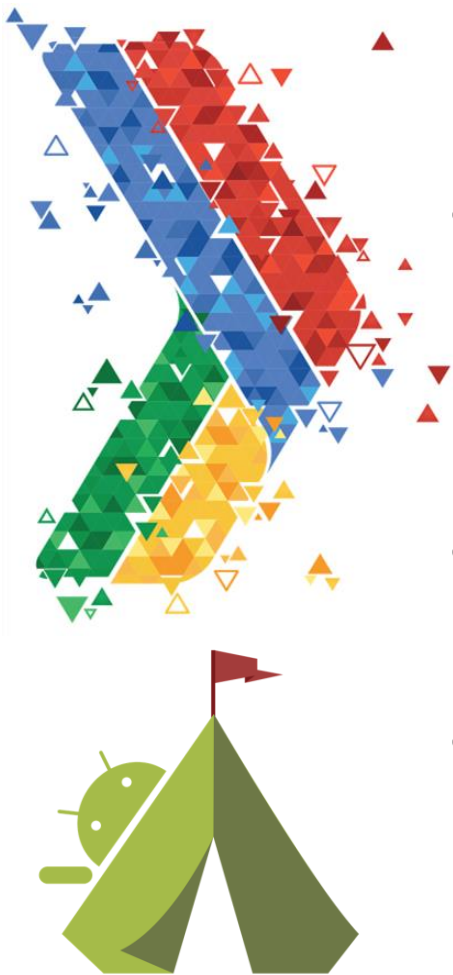
# Características (1/2)

- Extracción y decodificación automática de datos
- Extracción de datos de dispositivos no enraizados sin dispositivos por Android Backup (versiones de Android 4.x)
- Extracción de datos con permisos de raíz: root ADB daemon, modo de recuperación CWM o SU binary (Superuser / SuperSU)

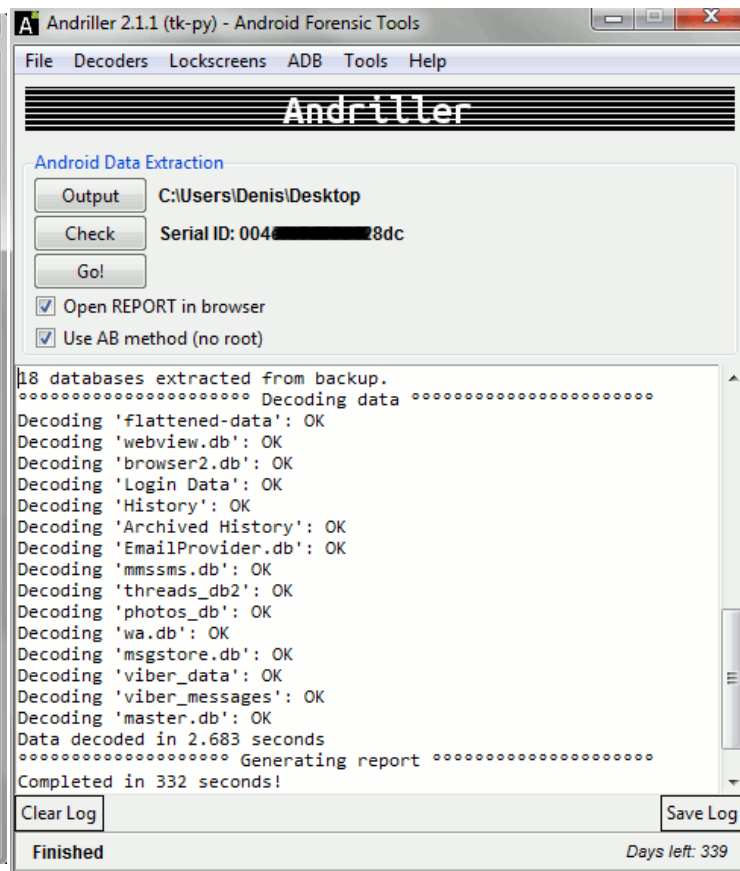
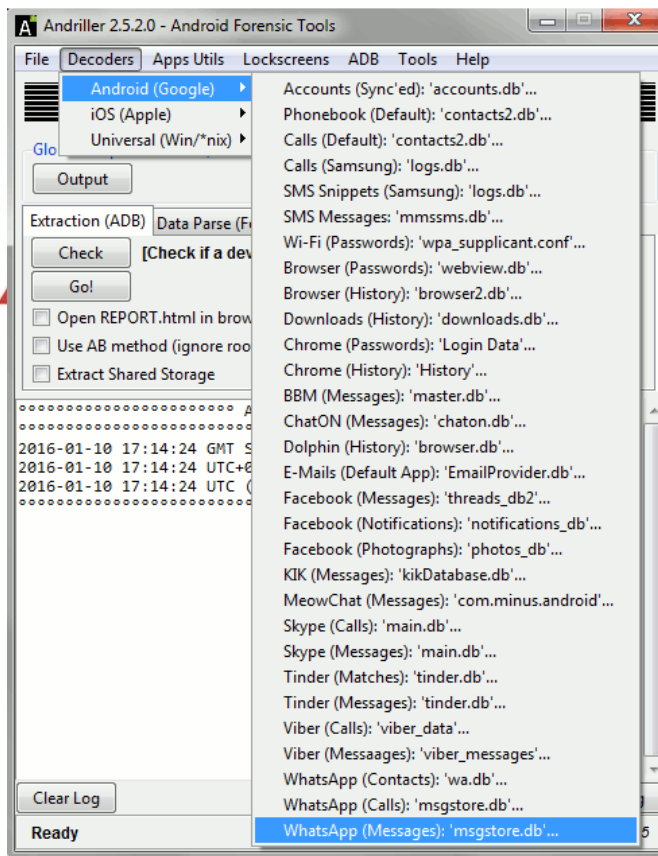


## Características (2/2)

- Análisis y descodificación de datos para la estructura de Carpetas, archivos Tarball (desde copias de seguridad de nanddroid) y Android Backup (archivos 'backup.ab')
- Selección de decodificadores de bases de datos individuales para Android y Apple
- Desencryptado de las bases de datos archivadas de WhatsApp cifradas

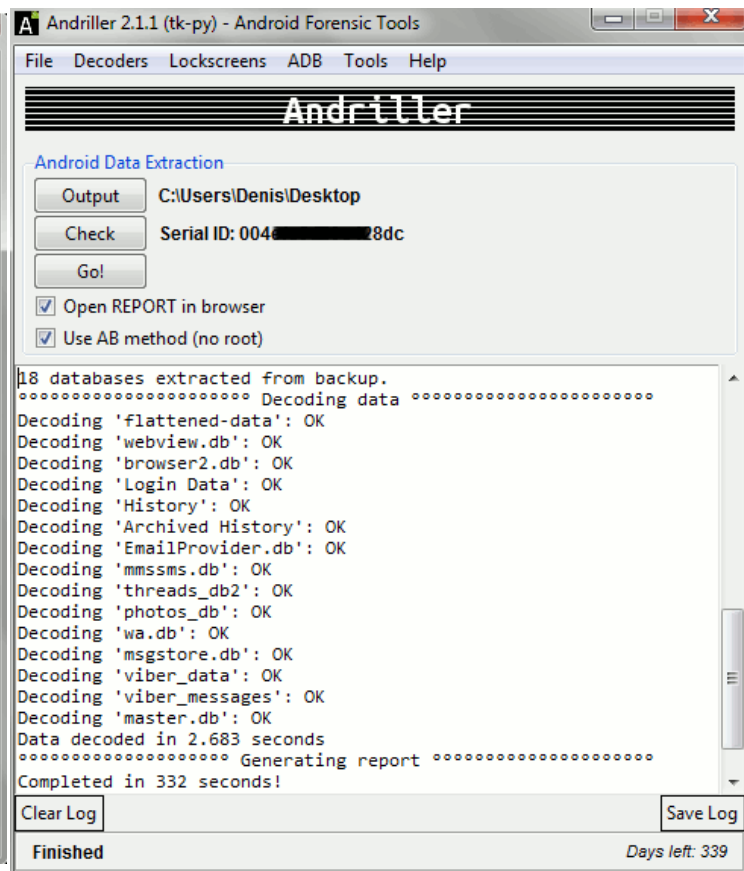
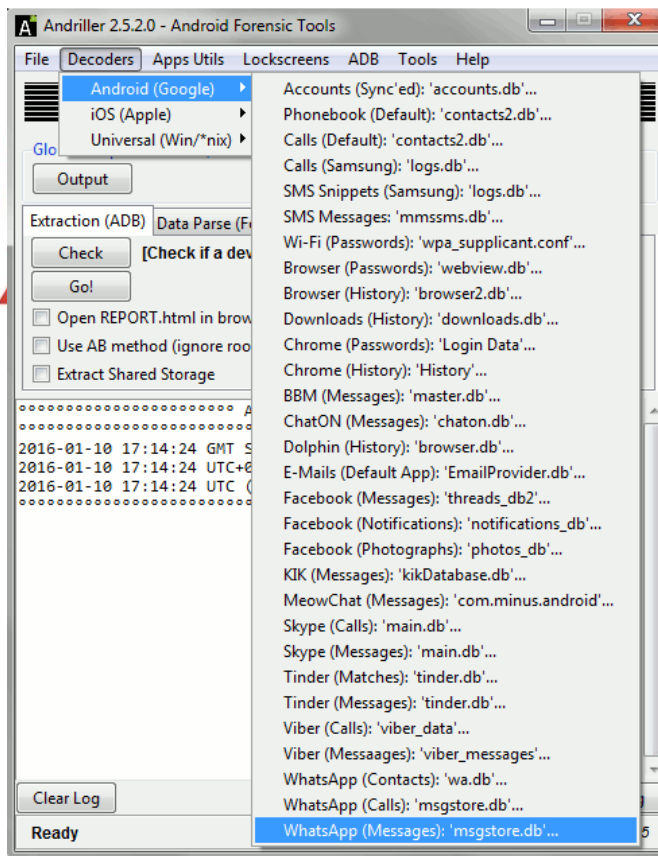


# Decodifica





# Decodifica



# Creación de informes

# This report was generated using Andriller version 2.0.5 on 2014-05-19 22:23:34 BST #

[Andriller Report] LGE Nexus 4 | IMEI:353[REDACTED]9

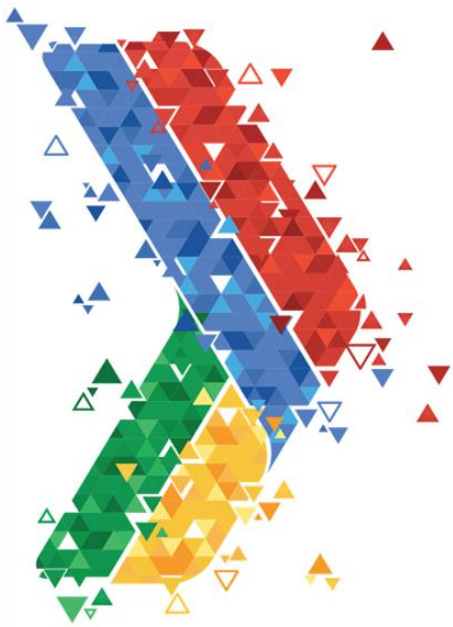
Type	Data	
ADB serial:	004[REDACTED]28dc	
Android ID:	e75[REDACTED]49ff	
Shell permissions:	root(su)	
Manufacturer:	LGE	
Model:	Nexus 4	
IMEI:	353[REDACTED]9	
Android version:	4.4.2	
Build name:	cm_mako-userdebug 4.4.2 KVT49L	
WiFi MAC:	10:68:3f:[REDACTED]3	Security (Lockscreen Pattern): [REDACTED]a8aac3d13[REDACTED]ee691b7d7b8[REDACTED]
Bluetooth MAC:	10:68:3f:[REDACTED]8	Security (Lockscreen Hash): [REDACTED]D44D56F694B475F898F53FDD9469E2AA48BD1EE62437E6FC8C159F8E1E598[REDACTED]
Bluetooth name:	DS Nexus 4	Security (Lockscreen Salt): [REDACTED]759467610083
Local time:	2014-05-19 22:23:34 BST	System: <a href="#">Synchronised Accounts (16)</a>
Android time:	2014-05-19 22:23:34 BST	System: <a href="#">Wi-Fi Passwords (100)</a>
Accounts:	com.google:[REDACTED]	Web browser: <a href="#">Android Web Browser: Passwords (2)</a>
	com.google:[REDACTED]	Web browser: <a href="#">Android Web Browser: History (38)</a>
	com.google:[REDACTED]	Web browser: <a href="#">Google Chrome: Passwords (49)</a>
	com.skype.contacts.sync:[REDACTED]	Web browser: <a href="#">Google Chrome: History (1,913)</a>
	com.twitter.android.auth.login:[REDACTED]	Web browser: <a href="#">Google Chrome: Archived History (862)</a>
	com.twitter.android.auth.login:[REDACTED]	Android E-mail: <a href="#">E-mails (0)</a>
	com.evemote:[REDACTED]	Communications data: <a href="#">Contacts (978)</a>
	com.dropbox.android.account:[REDACTED]	Communications data: <a href="#">Call logs (500)</a>
	com.github:[REDACTED]	Communications data: <a href="#">SMS Messages (3,341)</a>
	com.bbm.account: BBM Groups	Applications data: <a href="#">Facebook: Messages (217)</a>
	com.linkedin.android:[REDACTED]	Applications data: <a href="#">Facebook: Viewed Photos (557)</a>
	com.facebook.auth.login:[REDACTED]	Applications data: <a href="#">Facebook: Notifications (30)</a>
	com.shazam.android: Sync	Applications data: <a href="#">WhatsApp Contacts (111)</a>
	com.whatsapp: WhatsApp	Applications data: <a href="#">WhatsApp Messages (2,569)</a>
	com.viber.voip.account:[REDACTED]	Applications data: <a href="#">Viber Messages (74)</a>
	Applications data: <a href="#">Blackberry Messenger (295)</a>	

# Equipo de análisis forense de móviles Cellebrite UFED Touch Ultimate

Permite la extracción, decodificación, análisis y generación de informes de datos móviles con la tecnología más avanzada.





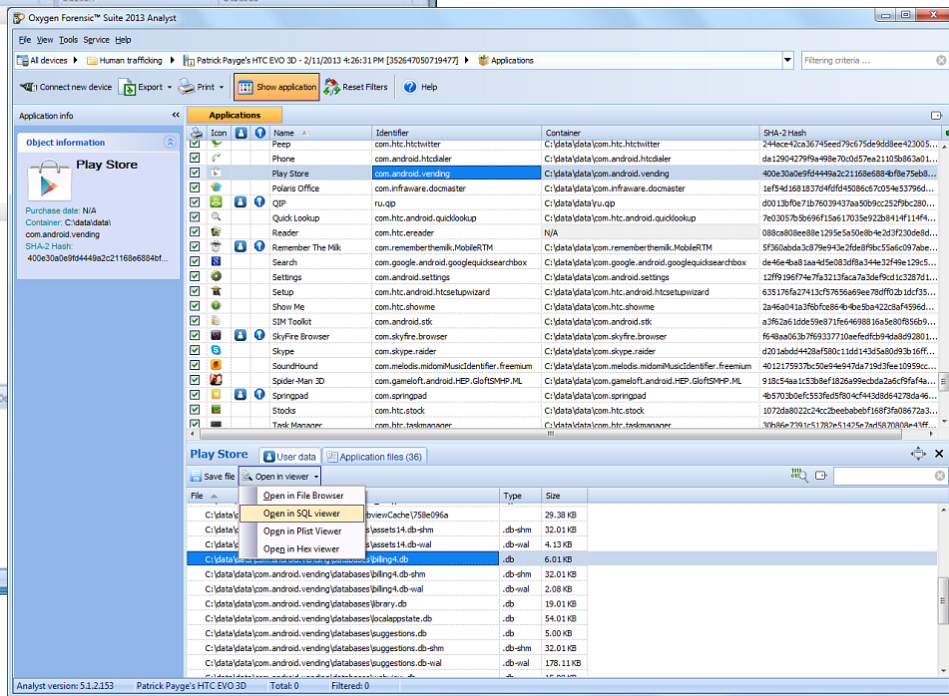


# Equipo de análisis forense de móviles MSAB Office

MSAB Office es un paquete completo que incluye las soluciones de XRY necesarias para que los investigadores puedan tener acceso a todos los métodos posibles para recuperar datos de un dispositivo móvil.



# OXYGEN FORENSIC

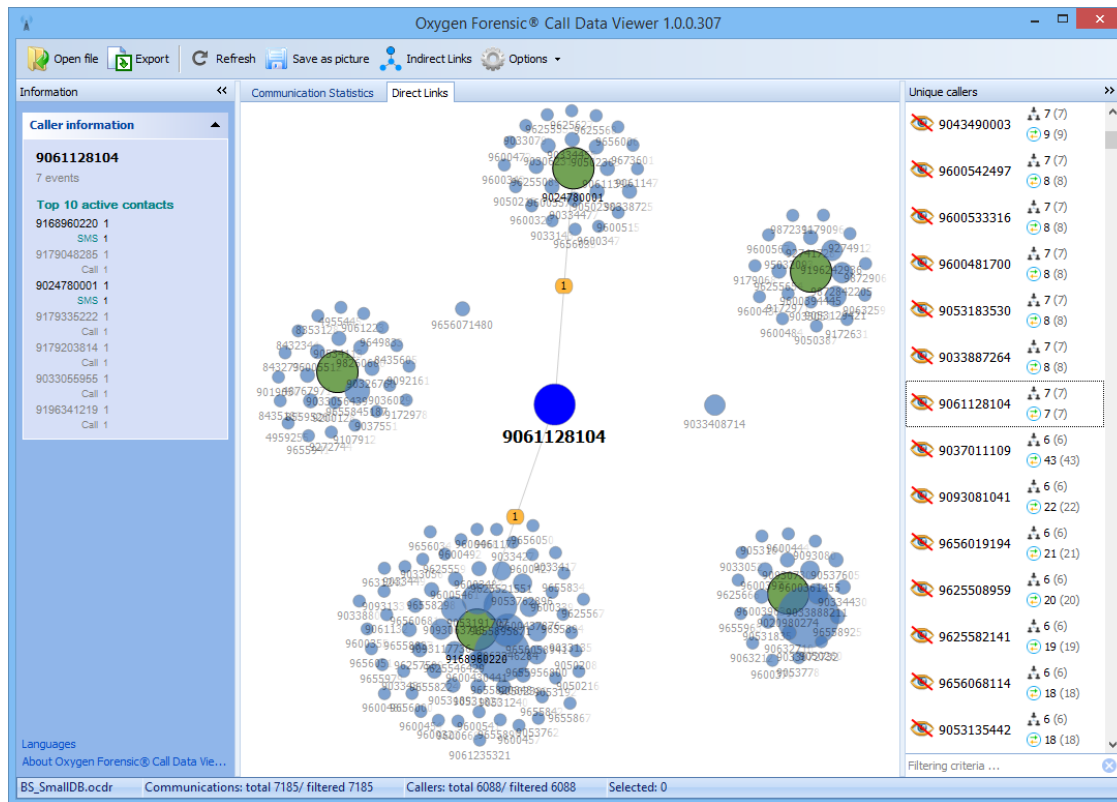


# OXYGEN FORENSIC ANALYST

- Adquiere los datos de 17310+ dispositivos (Android, BlackBerry, iOS, Windows Phone, etc..)
- Importaciones dispositivo backups & imágenes (iTunes, Android, JTAG y más)
- Analiza los datos de 410 aplicaciones únicas y 5540+ App versiones totales
- Recupera una amplia variedad de datos borrados
- Ofrece análisis de datos (Contactos Agregados, Grafo Social, Cronología)
- Exporta datos a formatos de archivo populares, como PDF, RTF, XLS,XML, etc..



# OXYGEN FORENSIC



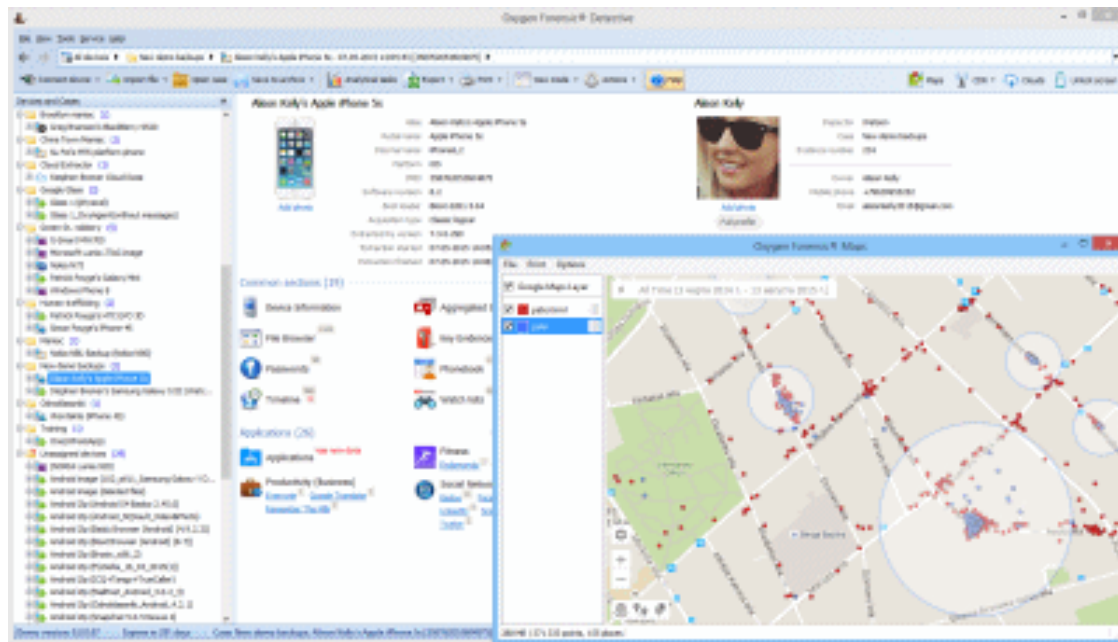


# OXYGEN FORENSIC DETECTIVE

- Incluye toda la funcionalidad de Oxygen Forensic® Analyst
- Encuentra contraseñas para backups y las imágenes cifradas
- Desactiva el screen lock en los dispositivos Android OS populares
- Permite extraer datos de servicios del cloud.
- Importaciones y registros de datos de llamadas analizadas
- Incluye utilidad de mapeo geo avanzada



# OXYGEN FORENSIC DETECTIVE





## Contactos:



[clara.flores.s@gmail.com](mailto:clara.flores.s@gmail.com)



[cfs.codev@gmail.com](mailto:cfs.codev@gmail.com)



ClaritaFlor



ClaraFloresS



ClaritaFlor



ClaritaFlor



ClaritaFlor





**GRACIAS !!!**

