



---

# Forensia dispositivos móviles

Roberto Gómez Cárdenas  
ITESM-CEM  
rogomez@itesm.mx

Lámina 1 Dr. Roberto Gómez Cárdenas



# Introducción

---

- La gente almacena bastante información en teléfonos celulares y dispositivos móviles.
- Información almacenada en dispositivos móviles
  - Llamadas
  - Mensajes SMS
  - Correo electrónico
  - IM
  - Páginas Web
  - Fotos

Lámina 2 Dr. Roberto Gómez Cárdenas



## Introducción

---

- Información almacenada
  - Calendarios personales
  - Directorio
  - Archivos de música
  - Grabaciones de voz
- Investigar teléfonos celulares y dispositivos móviles es uno de los tareas más retadoras en forensia digital.

Lámina 3 Dr. Roberto Gómez Cárdenas



## Aspectos básicos telefonía móvil

---

- Tecnología ha avanzado de forma muy rápida.
- Tres generaciones de teléfonos móviles.
  - Análogos
  - Digital personal communications service (PCS)
  - Tercera generación (3G)
    - Ofrece un ancho de banda más grande
- Varias redes digitales son usados en la industria de la telefonía móvil.

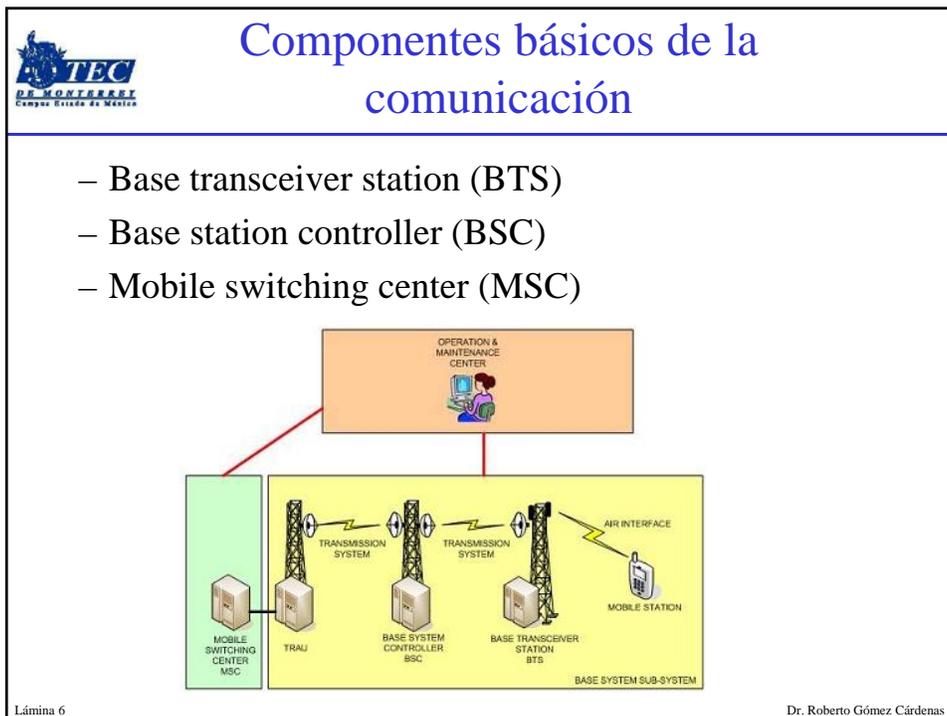
Lámina 4 Dr. Roberto Gómez Cárdenas



## Características redes digitales

Red digital	Descripción
Code Division Multiple Access	Esta tecnología, desarrollado durante la Segunda Guerra Mundial, fue patentada por Qualcomm después de la guerra. Una de las redes más comunes, usa el espectro completo de frecuencias de radio para definir canales. Sprint y Verizon usan CDMA.
Global System for Mobile Communications (GSM)	Es la otra red digital más común. Es usada por Cingular AT&T y T-Mobile; y es el estándar en Europa y Asia.
Time Division Multiple Access (TDMA)	Esta red digital se refiere a la técnica de dividir una radio frecuencia en time slots; GSM usa dicha técnica. También se refiere a un estándar específico de red celular cubierto por Interim Standard (IS) 136.
Integrated Digital Enhanced Network (iDEM)	Este protocolo patentado fue desarrollado por Motorola. Combina diversos servicios, incluyendo la transmisión de datos, en una red.
Digital Advanced Mobile Phone Service (D-AMPS)	Esta red es una versión digital de estándar analógico original para celulares.
Enhanced Data GSM Environment (EDGE)	Esta red digital, una versión rápida de GSM, es designada para entregar datos.

Lámina 5
Dr. Roberto Gómez Cárdenas





## Dentro de los dispositivos móviles

---

- Abarca desde los simples teléfonos a computadoras pequeñas.
  - También conocidos como teléfonos inteligentes.
- Componentes hardware
  - Microprocesador, ROM, RAM, un pr



Lámina 7

Dr. Roberto Gómez Cárdenas



## Dentro dispositivos móviles

---

- Los datos se almacenan datos en EEPROM (Electrically Erasable Programmable Read-Only Memory)
  - Permite que los proveedores de servicio reprogramen teléfonos sin tener que acceder físicamente a los chips de la memoria.
- El Sistema Operativo se almacena en ROM
  - Memoria no volatil

Lámina 8

Dr. Roberto Gómez Cárdenas



## Tarjetas SIM (Subscriber Identity Module)

---

- Encontrado en las dispositivos GSM.
- Microprocesador y una EEPROM de 16KB a 4 MB.
- GSM se refiere a los teléfonos móviles como “estaciones móviles” y divide una estación en dos partes
  - La tarjeta SIM y el equipo móvil.
- Tarjetas SIM vienen en dos tamaños.
- La portabilidad de información hace a las tarjetas SIM versátiles.

Lámina 9 Dr. Roberto Gómez Cárdenas



## Propósitos SIM

---

- Identifica al subscriptor con la red.
- Almacena información personal.
- Almacena libreta de direcciones y mensajes.
- Almacena información relacionada con el servicio.

Lámina 10 Dr. Roberto Gómez Cárdenas



## PDAs

- Personal Digital Assistants
  - Eran dispositivos diferentes de los teléfonos móviles.
  - La mayor parte de los usuarios los cargan en lugar de una laptop.
- PDAs contienen un microprocesador, flash ROM, RAM y varios componentes hardware.
- El monto de información en un PDA varia dependiendo del modelo.
- Usualmente, es posible “sacar” el calendario, libreta de direcciones, acceso a Web y otros datos.

Lámina 11 Dr. Roberto Gómez Cárdenas



## Características PDAs

- Tarjetas de memoria periférica son usados con PDAs.
  - Compact Flash (CF)
  - MultiMedia Card (MMC)
  - Secure Digital (SD)
- La mayor parte de los PDAs se sincronizan con una computadora.
  - Se cuentan con slots para dicho propósito.

Lámina 12 Dr. Roberto Gómez Cárdenas



## Adquisición datos en dispositivos móviles

---

- Las mayores preocupaciones con dispositivos móviles son la pérdida de potencia y sincronización con PCs.
- Todos los dispositivos móviles cuentan con memoria volátil.
  - Asegurarse que no se pierde energía eléctrica antes de obtener datos de la RAM.
- Dispositivo móvil atado a la PC vía un cable debe ser desconectado de la PC inmediatamente.
- Dependiendo de la orden, y/o el caso, el tiempo de levantamiento de información puede ser importante.

Lámina 13
Dr. Roberto Gómez Cárdenas



## Aislar el dispositivo

---

- Es posible que mensajes sean recibidos en el dispositivo móvil después de la toma de datos.
- Aislar el dispositivo de señales de entrada con alguna de las siguientes opciones.
  - Poner del dispositivo dentro de una lata de pintura (vacía).
  - Usar una bolsa Paraben Wireless StrongHold.
  - Usar 8 niveles de bolsas antiestáticas para bloquear la señal.
- Desventaja aislado: dispositivo móvil se pone en modo roaming
  - Acelera el drenado de batería.



Lámina 14
Dr. Roberto Gómez Cárdenas



## Analizando el dispositivo

---

- Verificar las siguientes áreas en el laboratorio forense
  - Memoria interna.
  - Tarjeta SIM
  - Remover tarjetas de memorias externas.
  - Servidor del sistema.
- Verificar servidores sistema requiere una orden emitida por el juez.
- Sistema de archivos de la tarjeta SIM cuenta con una estructura jerárquica.

Lámina 15
Dr. Roberto Gómez Cárdenas



## Estructura sistema archivos SIM

---

```

graph TD
    MF[MF] --- DF_GSM[DF GSM]
    MF --- DF_DCS[DF DCS 1800]
    MF --- DF_Telecom[DF Telecom]
    MF --- EF_1[EF]
    DF_GSM --- EF_2[EF]
    DF_GSM --- EF_3[EF]
    DF_DCS --- EF_4[EF]
    DF_Telecom --- EF_5[EF]
    EF_1 --- EF_6[EF]
            
```

MF: Master File  
 DF: Dedicated File  
 EF: Elementary File

Lámina 16
Dr. Roberto Gómez Cárdenas



## Información a obtener

---

- Datos relacionados con el servicio
  - Identificadores de la tarjeta SIM y el suscriptor.
- Datos llamadas, como números marcados.
- Información sobre mensajes enviados.
- Información sobre ubicación
- Nota:
  - Si la energía se pierde, es posible que se requieran PINs y/u otros códigos de acceso para ver los archivos.

Lámina 17 Dr. Roberto Gómez Cárdenas



## Equipo de forensia móvil

---

- Es algo relativamente nuevo.
- Mayor reto: cambio constante en los modelos de teléfonos celulares.
- Cuando se adquiere evidencia, generalmente se llevan a cabo dos tareas
  - Actuando como si se esta sincronizando con una PC
  - Leer la tarjeta SIM
- Primer paso es identificar el dispositivo móvil.

Lámina 18 Dr. Roberto Gómez Cárdenas



## Equipo de forensia móvil

---

- Asegurarse que se instaló el software del dispositivo móvil en la estación de trabajo forense.
- Conecte el teléfono a una fuente de energía y conecte los cables correctos.
- Después de conectar los dispositivos
  - Empieza el programa forense y comience a bajar la información disponible.

Lámina 19
Dr. Roberto Gómez Cárdenas



## Lectores tarjetas SIM

---

- Dispositivo que es una combinación de hardware/software usado para acceder a la tarjeta SIM.
- Necesario encontrarse en un laboratorio forense equipado con los dispositivos antiestáticos apropiados.
- El procedimiento general es el siguiente:
  - Remover el panel posterior del dispositivo.
  - Remover la batería.
  - Bajo la batería, quitar la tarjeta SIM de su ubicación.
  - Insertar la tarjeta SIM en el lector de tarjetas.




Lámina 20
Dr. Roberto Gómez Cárdenas



## Lectores tarjetas red

- Una variedad de lectores de tarjetas se encuentran en el mercado.
  - Algunos pueden usarse para forensia otros no.
- Documentar mensajes que aún no han sido leídos es crítico.
  - Usar una herramienta que tome fotos de cada screen.




Lámina 21 Dr. Roberto Gómez Cárdenas



## Lectores tarjetas red



Lámina 22 Dr. Roberto Gómez Cárdenas



## Herramientas computo forense móvil

- Difieren en los aspectos que despliegan y el nivel de detalle.
- Ejemplos de herramientas
  - SIMCon
  - Paraben Software Device Seizure Toolbox
  - BitPim
  - MOBILedit!
  - Data Pilot Secure View









Lámina 23

Dr. Roberto Gómez Cárdenas



## SIMCon: Vista Hexadecimal

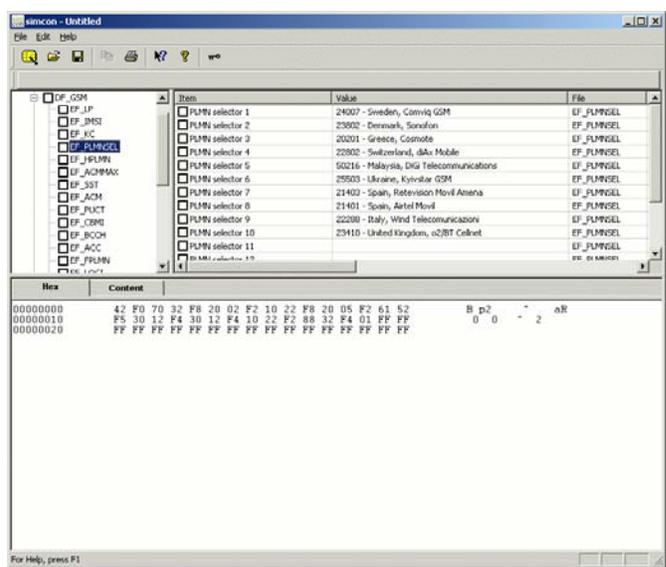
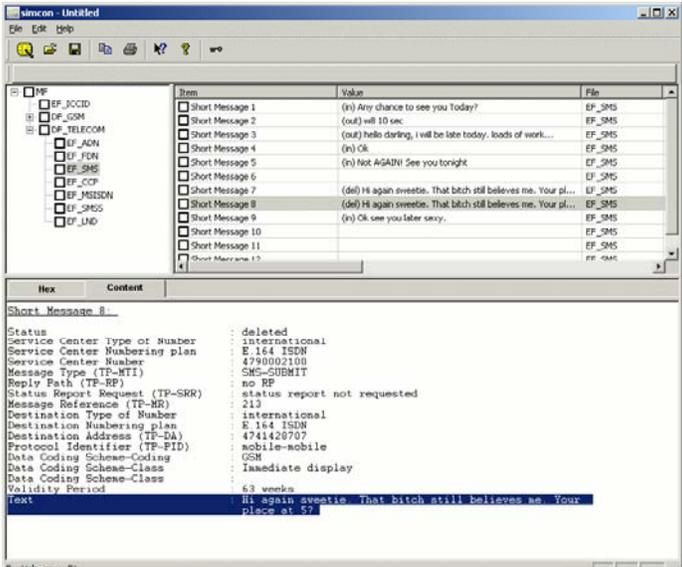


Lámina 24

Dr. Roberto Gómez Cárdenas



## SIMCon: Mensajes



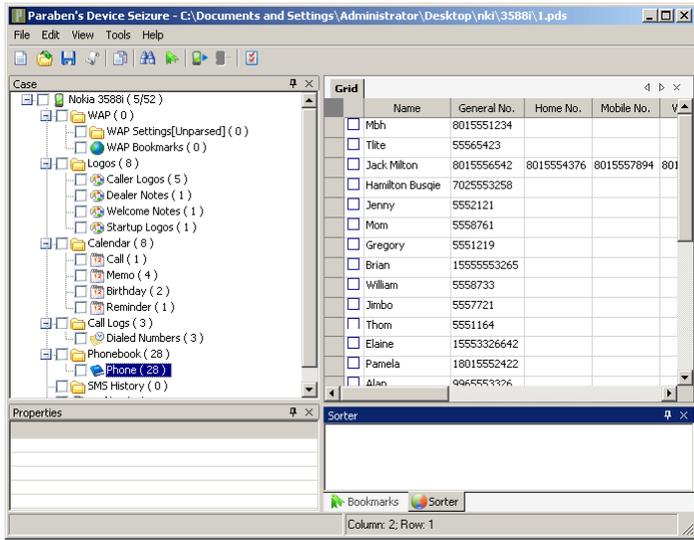
The screenshot shows the SIMCon application interface. On the left, there is a tree view of message folders including EF\_JCCID, EF\_GSM, EF\_TELECOM, EF\_AON, EF\_FON, EF\_SMS, EF\_CCF, EF\_MESSON, EF\_SMS, and EF\_LND. The main window displays a list of messages with columns for Item, Value, and File. Below this, the details for 'Short Message 8' are shown, including fields like Status, Service Center type of Number, Service Center Numbering plan, Service Center Number, Message Type (TP-MTI), Reply Path (TP-RP), Status Report Request (TP-SRR), Message Reference (TP-MR), Destination Type of Number, Destination Numbering plan, Destination Address (TP-D4), Protocol Identifier (TP-PID), Data Coding Scheme-Coding, Data Coding Scheme-Class, and Validity Period. The text of the message is visible at the bottom: 'Hi again sweetie. That bitch still believes in. Your place at 52'.

Lámina 25

Dr. Roberto Gómez Cárdenas



## Screenshot Paraben



The screenshot shows the Paraben software interface. The main window displays a grid of contact information. The grid has columns for Name, General No., Home No., and Mobile No. The data in the grid is as follows:

Name	General No.	Home No.	Mobile No.
Mbh	8015551234		
Tilte	55565423		
Jack Milton	8015556542	8015554376	8015557894
Hamilton Busque	7025553258		
Jenny	5552121		
Mom	5558761		
Gregory	5551219		
Brian	1555553265		
William	5558733		
Jimbo	5557721		
Thom	5551164		
Elaine	15553326642		
Pamela	18015552422		
Alan	9966553376		

The interface also shows a tree view on the left with folders like WAP Settings, Logos, Caller Logos, Dealer Notes, Welcome Notes, Startup Logos, Calendar, Call, Memo, Birthday, Reminder, Call Logs, Dialed Numbers, Phonebook, and Phone. The 'Phone' folder is currently selected.

Lámina 26

Dr. Roberto Gómez Cárdenas



## BitPim

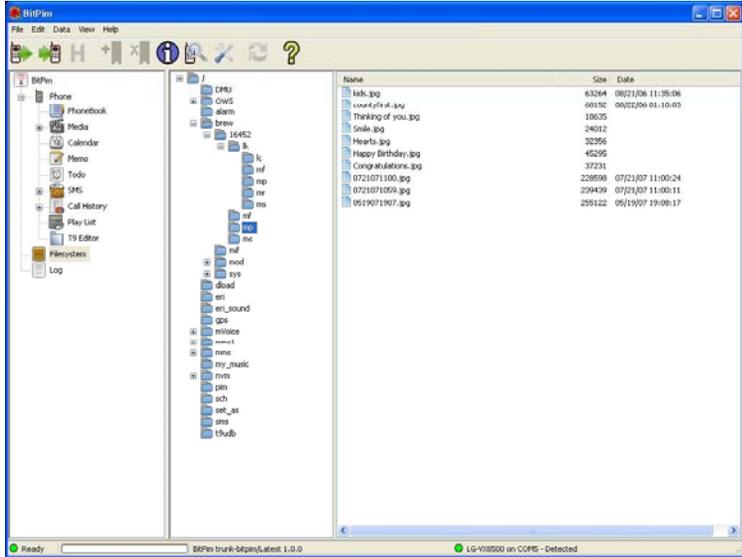


Lámina 27
Dr. Roberto Gómez Cárdenas



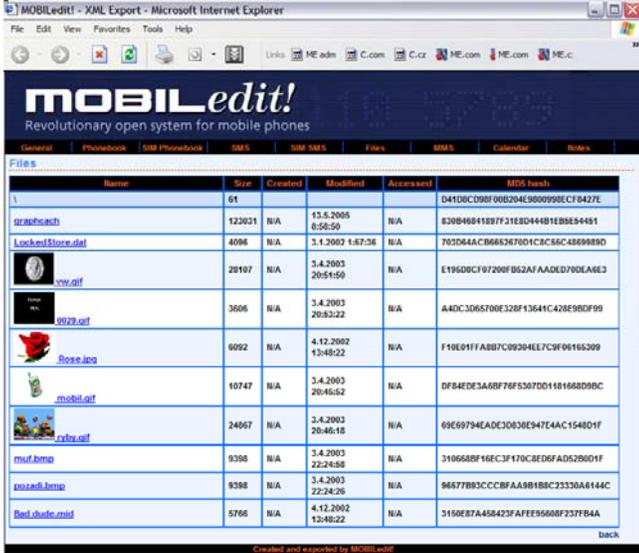
## MOBILedit!



Lámina 28
Dr. Roberto Gómez Cárdenas



# MOBILedit!



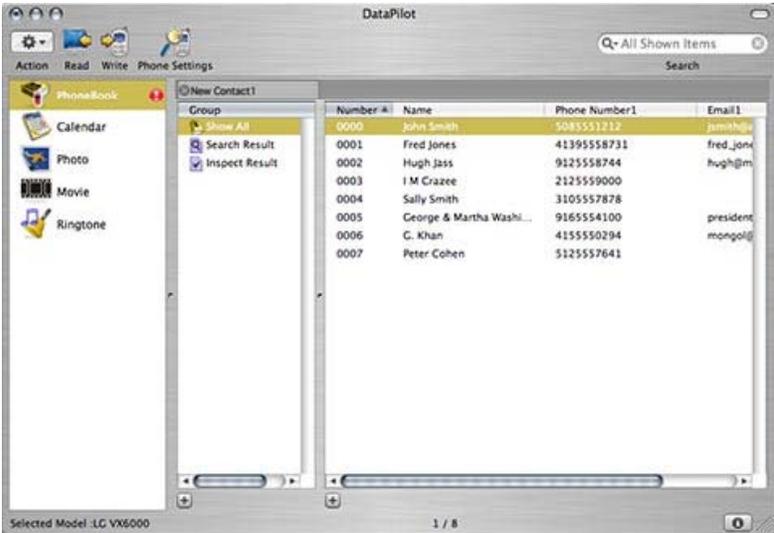
The screenshot shows the MOBILedit! XML Export interface. It features a table with the following data:

Name	Size	Created	Modified	Accessed	MD5 hash
1	61				D41D0C98F00B204E300998ECF0427E
grndfscash	122021	N/A	15.6.2005 0:58:59	N/A	820B48641897F31E8D44481E8E84481
LockedPhone.dat	4098	N/A	3.1.2003 1:57:38	N/A	703D64ACB662670D1C8C56C4B6989D
vw.gif	28107	N/A	3.4.2005 20:51:50	N/A	E195D8CF97200F852AF AADED700A8E3
6929.gif	3606	N/A	3.4.2003 20:83:22	N/A	A4DC3065700E320F13641C420E98DF99
Rose.jpg	6092	N/A	4.12.2002 13:48:22	N/A	F10E91FA8B7C09204EE7C9F06166209
mobil.gif	10747	N/A	3.4.2003 20:46:52	N/A	DF84EDE3A60F78F5307D01181668D99C
xyby.gif	24067	N/A	3.4.2003 20:46:18	N/A	69E69794EADC3D630E947E4AC1548D1F
muf.bmp	9368	N/A	3.4.2003 22:24:58	N/A	3106688F16EC3F170C8ED6FAD5280D1F
pozati.bmp	9388	N/A	3.4.2003 22:24:26	N/A	96577893CC8FAA981B8C33330A8144C
bad_chute.msd	5766	N/A	4.12.2002 13:48:22	N/A	3150E87A458423FAFE95680F237FB4A

Lámina 29 Dr. Roberto Gómez Cárdenas



# DataPilot



The screenshot shows the DataPilot software interface. It features a table with the following data:

Number	Name	Phone Number1	Email1
0000	John Smith	5085552112	jsmith@u...
0001	Fred Jones	41395558731	fred_jon...
0002	Hugh Jass	9125558744	hugh@m...
0003	I M Crazee	2125559000	
0004	Sally Smith	3105557878	
0005	George & Martha Washi...	9165554100	preside...
0006	G. Khan	4155550294	mongol@...
0007	Peter Cohen	5125557641	

Lámina 30 Dr. Roberto Gómez Cárdenas