Forensia dispositivos móviles

Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx

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

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 análogo 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

Componentes básicos de la comunicación

- Base transceiver station (BTS)
- Base station controller (BSC)
- Mobile switching center (MSC)

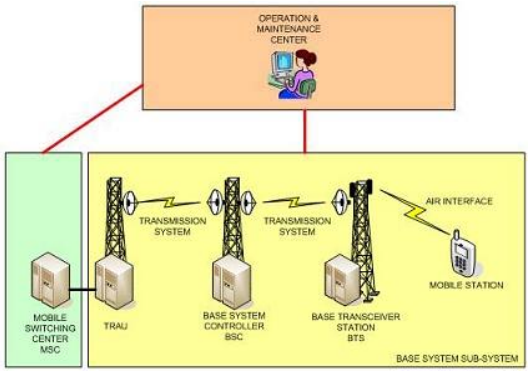


Lámina 6 Dr. Roberto Gómez Cárdenas

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 (Electronically 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 Indentity 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 perdida 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.

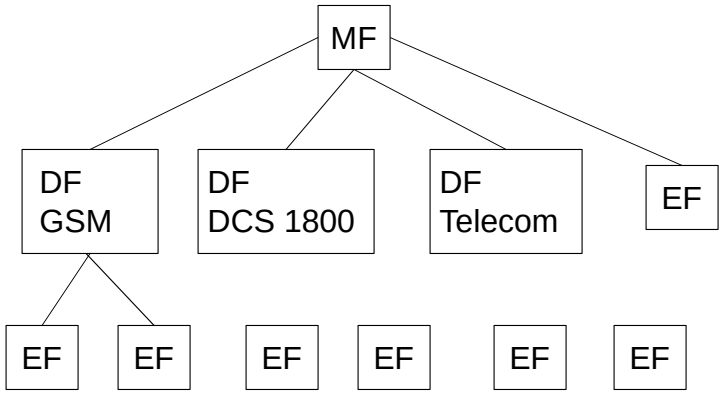
Lámina 14 Dr. Roberto Gómez Cárdenas

Analizando el dispositivo

- Verificar las siguientes área 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



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 subscriptor.
- 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

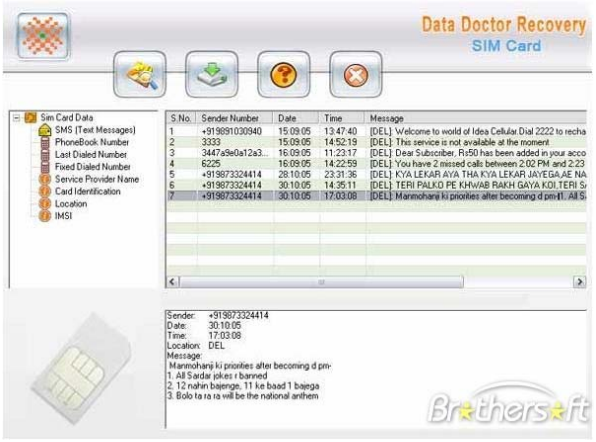


Lámina 22 Dr. Roberto Gómez Cárdenas

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

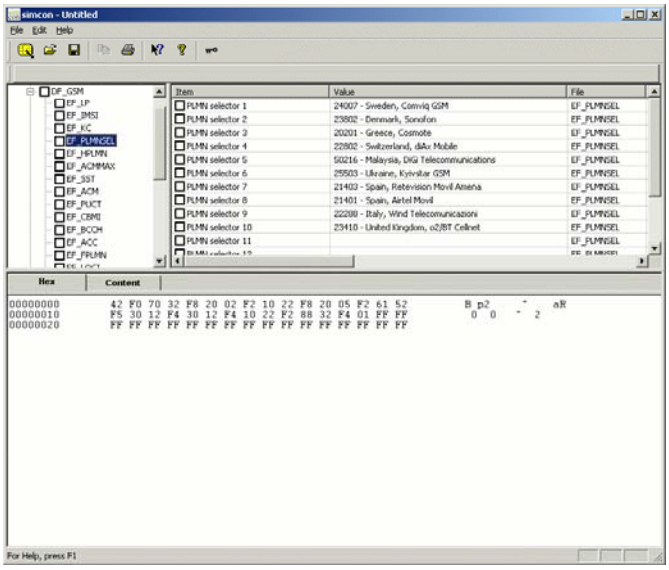
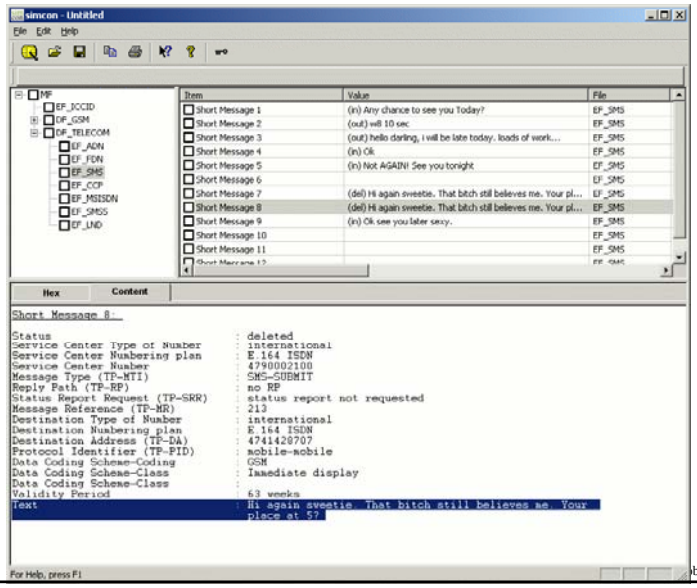
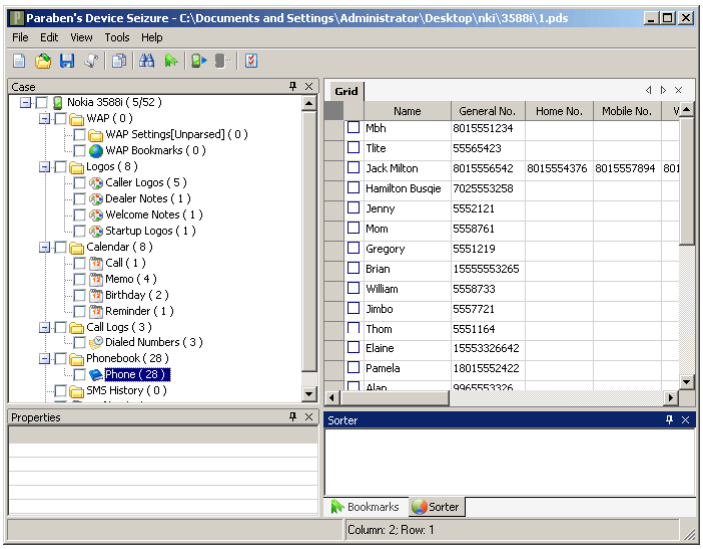


Lámina 24 Dr. Roberto Gómez Cárdenas

SIMCon: Mensajes



Screenshot Paraben



BitPim

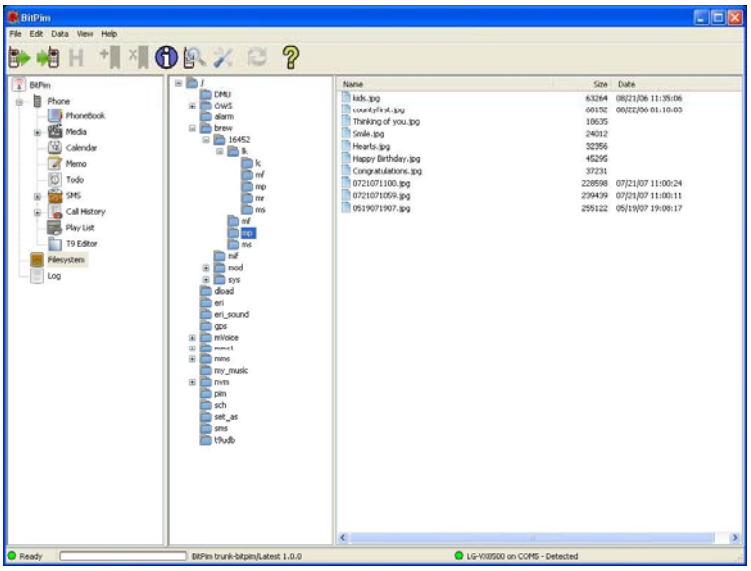


Lámina 27 Dr. Roberto Gómez Cárdenas

MOBILedit!

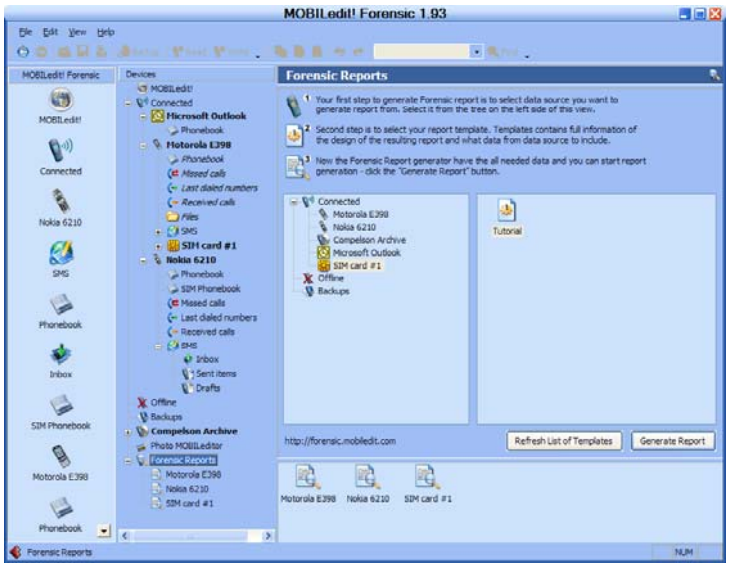


Lámina 28 Dr. Roberto Gómez Cárdenas

MOBILedit!

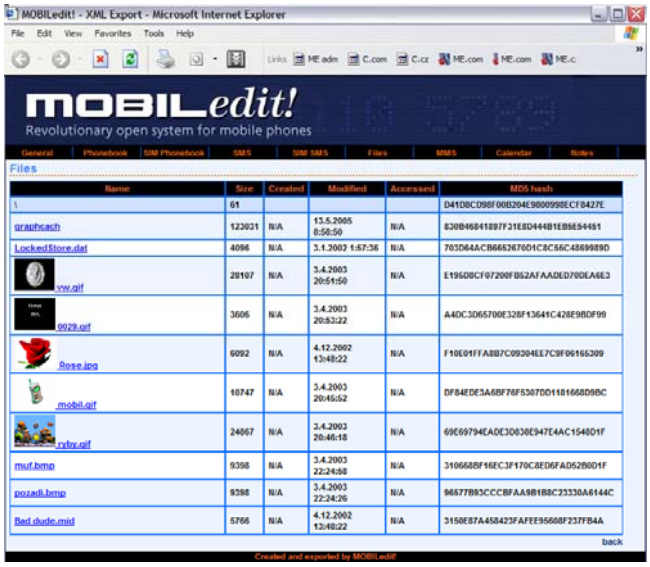


Lámina 29 Dr. Roberto Gómez Cárdenas

DataPilot

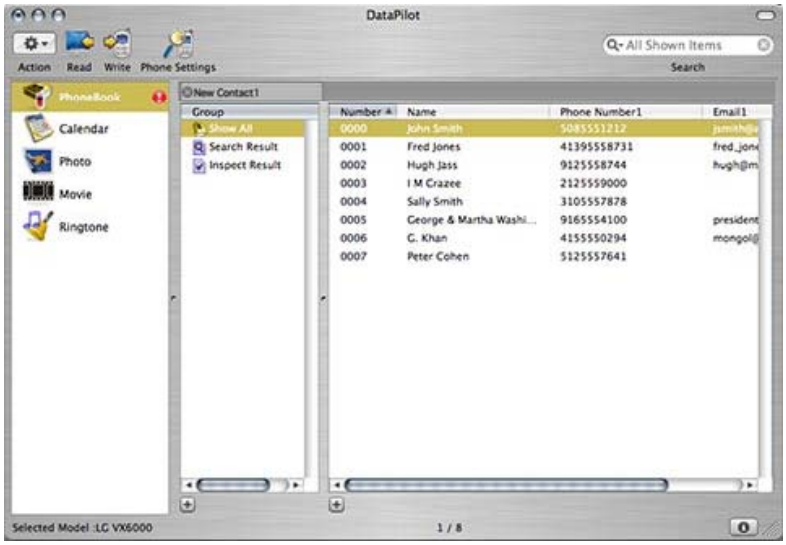


Lámina 30 Dr. Roberto Gómez Cárdenas