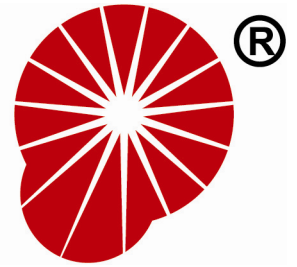


susteen



Mobile Forensics

Presented By :

Javier Martinez
“The Wireless Evangelist”



Agenda

- Introduction
- The Wireless Industry Today
- Mobile Forensics Today
 - The subscriber
 - The mobile station
 - The network
- The Roadmap to Mobile Forensics
- Demo
- Q & A

Who we are?



Business Highlights

- Founded in 1992
- Incorporated in California
- 100% privately owned
- DataPilot US market leader with 95% market share in 2004-2007 (NPD)
- Largest no. of US cell phones supported (600+ handsets as of 06/07)
- Single Point Vendor (software and hardware)



Who I am?



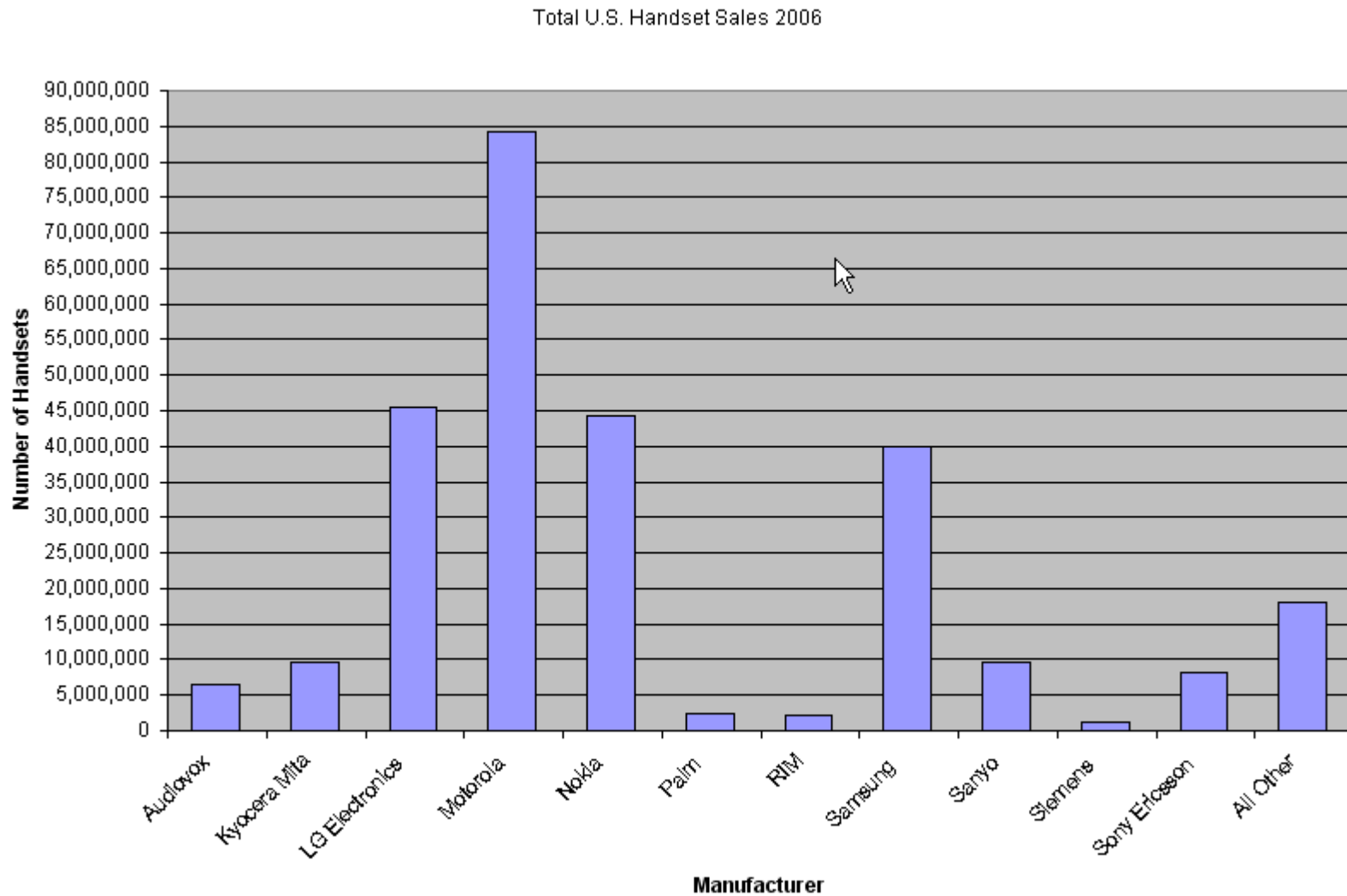
The Wireless Industry Today



- Total number of handsets sold in the U.S in 2006 was 271,789,450.
- Total number of subscribers in the U.S. in 2006 was 233,040,781.
- What does this mean?



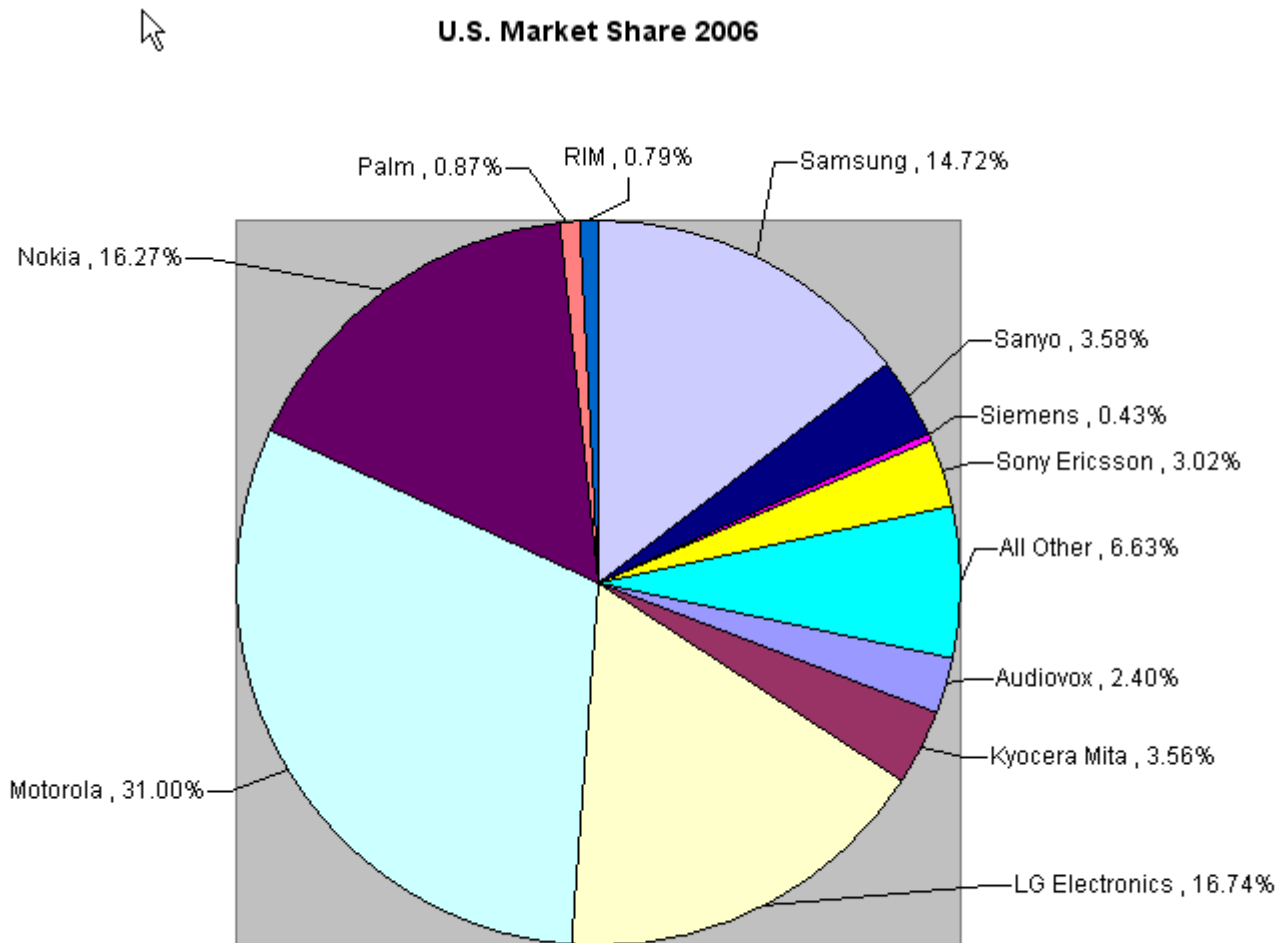
2006 Handset Sales



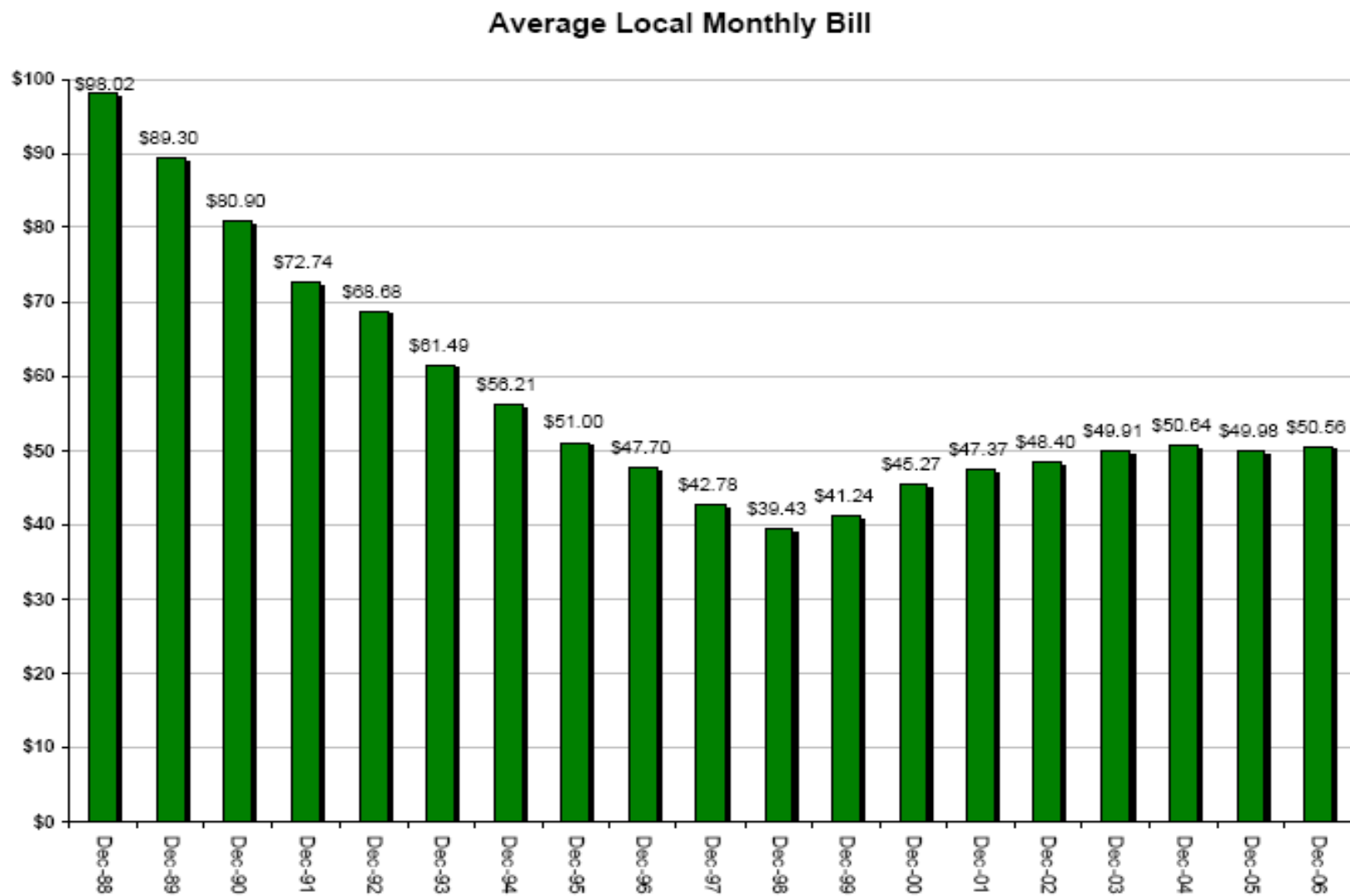
Source: NPD



U.S. Market Share 2006



Average Local Monthly Bill



Average Local Monthly Bill Grows 1.2% Year-over-Year

Source: CTIA

Materials May not be reproduced or photocopied in any form without written permission from CTIA

© 2006 CTIA-The Wireless Association®



Mobile Forensics Today



The Tools

Today: you need multiple tools to do the job. At the end of the day; the job is not done completely.

The tools you need, need to cover the following products:

- CDMA Phones
- GSM Phones
- External Memory Cards
- SIM Cards



Need to Understand

- How do we separate the subscriber and the equipment identities?
- What evidence can be obtained from the network entities?
 - Mobile Station (Cell Phone)
 - The Subscriber Identity Module (SIM)
 - The core network
- What tools can be used to extract the data without prejudice?
- The separation between the subscriber and the equipment as network entities
- How to present the evidence



The Subscriber



How to Identify a Subscriber

- Every mobile subscriber is issued with a smart card called a Subscriber Identity Module (SIM)
- As physical evidence the SIM provides details printed on the surface of;
 - Name of the Network Provider
 - Unique ID Number





Generic Properties

- All MS's have follow GSM standards on how they access and communicate with the network and SIM card
- Every MS has a unique ID called the International Mobile Equipment Identity (IMEI)
- Everything else is manufacturer dependent
 - File system
 - Features
 - Interface
 - Etc.
- Have to request the SIM PIN if activated
- May have optional MS PIN
 - No way of bypassing the MS PIN without specialist hardware provided by manufacturer



Electronic Access to the SIM

- Every SIM can be protected by a Personal Identification Number (PIN)
 - Set at point of manufacture
 - Can be changed by the Subscriber
 - Four digit code
 - Usually 3 attempts before phone is blocked
- Bypassing the PIN requires the Pin Unblocking Key (PUK)
 - 8 digit code
 - Set by manufacturer
 - Maximum 10 attempts before phone is permanently blocked



What Can Be Extracted From A SIM?

- A SIM is a smart card it has
 - A processor
 - Non-volatile memory
- Processor is used for providing access to the data and security
- GSM standard 1111 specifies the physical and logical properties of access mechanism for the SIM
- To access the data need;
 - Standard smart card reader
 - SIM access Software
- Data stored in binary files



An Example of SIM Data



SIM Card Report.html

- *Sample extracted using SIMIS*



What Can Be Extracted From A SIM?

- There is a fix number of files stored on a SIM
- Most have evidentiary value
 - However, most provide network rather than subscriber data
 - Most network data is not visible to the user of the SIM via the MS
- We shall concentrate on the user data files



Location Information File

File	Purpose	Size
LOCI	Location Information	11 bytes

- The bytes 5-9 of the LOCI contain the network Location Area Identifier (LAI) code
- Network Operator specific
- This data is retained when the MS is powered down
- Updated as MS moves from one location to another
- Analyst can determine which location the MS was present in when last used
- Location Areas can contain many cells
- LOCI DOES NOT DETAIL WHICH CELL!
- Cell data not stored on SIM



Serial Number

File	Purpose	Size
ICCID	Serial Number	10 bytes

- Integrated Circuit Card Identifier
- Corresponds to the number printed on the surface of the SIM
- Identifies the SIM



Subscriber Identifier

File	Purpose	Size
IMSI	Subscriber ID	9 bytes

- International Mobile Subscriber Identity
- Unique ID for every subscription on the Operator's network



Phone Number

File	Purpose	Size
MSISDN	Phone Number	variable

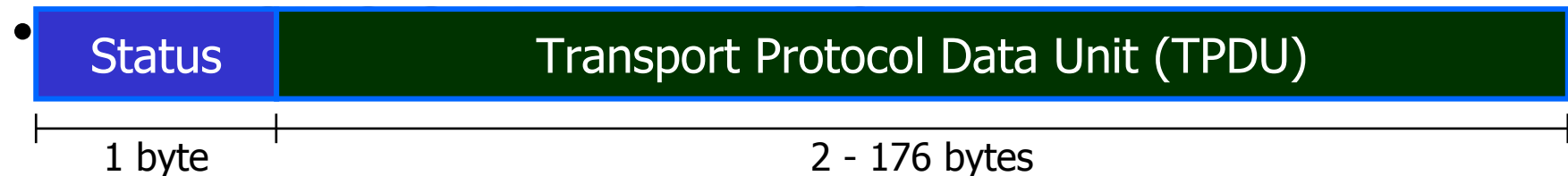
- Mobile Station International ISDN number



Text Message Data (SMS)

File	Purpose	Size
SMS	The text messages	$n * 176$ bytes
SMSP	Message parameters	variable
SMSS	Status of the message	variable

- Short Message Service is a popular communication method
- Most SIM's have a standard set of slots for storing messages.
 - Modern MS's allow storage on the device as well





Text Message Data (SMS) - Status

- Status byte values

Value	Interpretation
00000000	Unused
00000001	Mobile terminated message, read
00000011	Mobile terminated message, unread
00000101	Mobile originated message, sent
00000111	Mobile originated message, not sent

- When user deletes a message only the status flag is changed
 - Therefore, providing the message has not been overwritten any message in a slot can be recovered and translated using software



Dialled Numbers

File	Purpose	Size
AND	Short Dialled Numbers	variable

- Most SIMs have up to 100 slots for storing phone numbers
- Newer SIMs can store more than 100 slots
- Binary encoded name/number pair
- When number is deleted the slot is filled with FF hex value so deleted numbers cannot be retrieved forensically
- Slots are allocated in sequence
 - Therefore can forensically analyse if a number between two numbers has been deleted



Dialled Numbers

File	Purpose	Size
LND	Last Dialled Numbers	variable

- SIMs can store up to five of the last dialled numbers
- Binary encoded format
- Most MS manufacturers do not use this feature preferring to implement this feature on the MS calling logs
- NOTE: The SIM does not store received call data



The Equipment



Accessing MS Data

- Stored in flash memory
- Forensic Investigator must ensure the retrieval of data without alteration!
 - Imaging
 - As most MS's now have flash upgradeable Operating Systems, etc. this is usually a straightforward process
 - However, manufacturer's are reluctant to provide access to the tools to achieve this
 - Independent tools known as **Flashers** are available for most mainstream MS's but have no recognised legal status in some parts of the world.
 - Data suites
 - Provided by manufacturers
 - Allow access to SMS/MMS, call registers, phonebooks, etc. as stored on phone
 - Cannot access memory directly



Flash Memory

- Flash memory stores information in an array of [floating-gate transistors](#), called "cells". In traditional **single-level cell (SLC)** devices, each cell stores one bit of information. Some newer flash memory, known as **multi-level cell (MLC)** devices, can store more than one bit per cell by choosing between multiple levels of electrical charge to apply to the floating gates of its cells.
- On Mobile Phones: flash memory contains vital personal information and cellular operator information that constantly changes.



MS Data

- Very much dependent on the model, MAY include;
 - IMEI
 - Short Dial Numbers
 - Text/Multimedia Messages
 - Settings (language, date/time, tone/volume etc)
 - Stored Audio Recordings
 - Stored images/multimedia
 - Stored Computer Files
 - Logged incoming calls and dialled numbers
 - Stored Executable Programs (eg J2ME)
 - Stored Calendar Events
 - IxRTT, EvDO, GSM, GPRS, WAP and Internet settings



Threats to MS Data

- Tools such as Flashers and Data Suites can be used to directly manipulate MS data
 - Common threat is removing the Service Provider Lock (SP-Lock) limiting the MS to a single networked
 - Changing the IMEI on stolen phones
 - Networks blacklist stolen IMEI's in the EIR
 - Can also be used to avoid tracing an MS
 - Detecting changes to the IMEI
 - Compare the electronic IMEI with that printed on the inside of the device
- No scientific way to detect if flash memory has been flashed and if so why



The Network



Network Operator Data

- The Network Operators can provide detailed data on calls made/received, message traffic, data transferred and connection location/timing
- The HLR can provide;
 - Customer name and address
 - Billing name and address (if other than customer)
 - User name and address (if other than customer)
 - Billing account details
 - Telephone Number (MSISDN)
 - IMSI
 - SIM serial number (as printed on the SIM-card)
 - PIN/PUK for the SIM
 - Subscriber Services allowed
- Not necessarily for pre-pay!



The Call Data Records (CDR's)

- Produced in the originating MSC transferred to the OMC
 - Every call
 - Every message
- Each CDR contains;
 - Originating MSISDN
 - Terminating MSISDN
 - Originating and terminating IMEI
 - Duration of call
 - Type of Service
 - Initial serving Base Station (BTS)



A Reference Website

www.MobileForensicsCentral.com is a website where anyone can see all mobile forensic products. Anyone can see what product supports what phone and feature.



The Roadmap to Mobile Forensics



DEMO



Questions?

Partnering for Success



Javier Martinez

Director of Sales

susteen ®

8001 Irvine Center Drive, Ste. 1500

Irvine, CA 92618

Phone: (949) 789-8221

Email: Jmartinez@Susteen.com

Web Site: <http://www.Susteen.com>