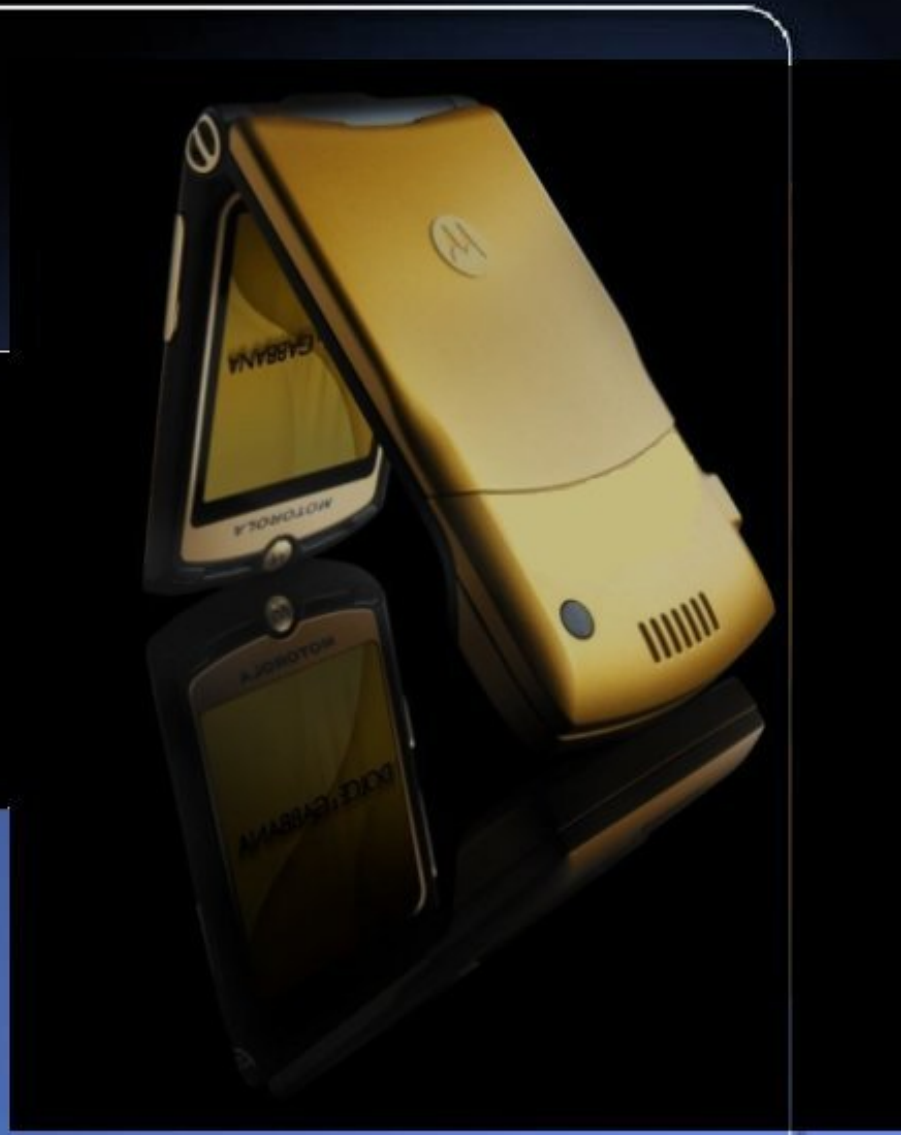
Mobile Device Forensics

Richard Ayers



Disclaimer

Certain commercial entities, equipment, or materials may be identified in this presentation in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

NIST
National Institute of Standards and Technology

Agenda

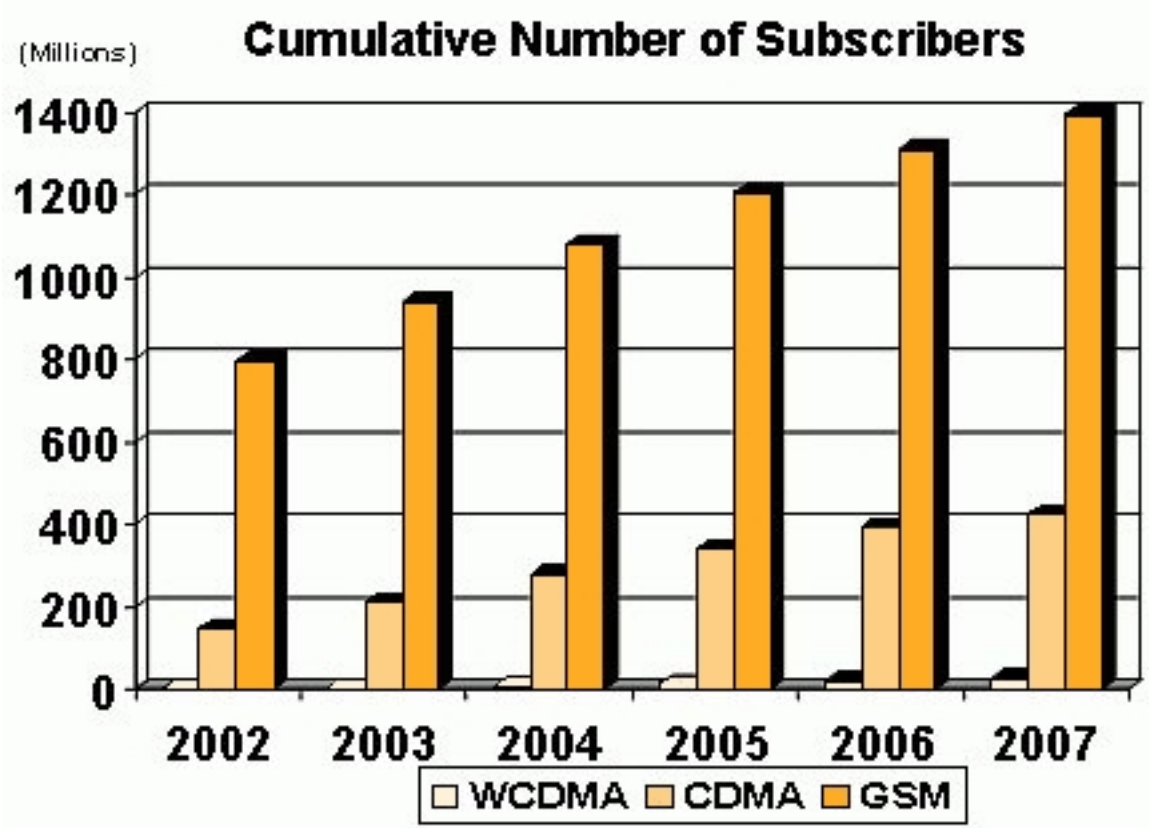
- Overview
- Tools and Devices
- Device Architecture
- Preservation
- Acquisition
- Digital Evidence
- Tool Validation
- Requirements
- Conclusions

Introduction

- Mobile devices are an evolving form of computing, used widely for personal and organizational purposes
- These compact devices are useful in managing information, such as contact details and appointments, corresponding electronically, and conveying electronic documents
- Over time, they accumulate a sizeable amount of information about the owner
- When involved in crimes or other incidents, proper tools and techniques are needed to recover evidence from such devices and their associated media

Motivation

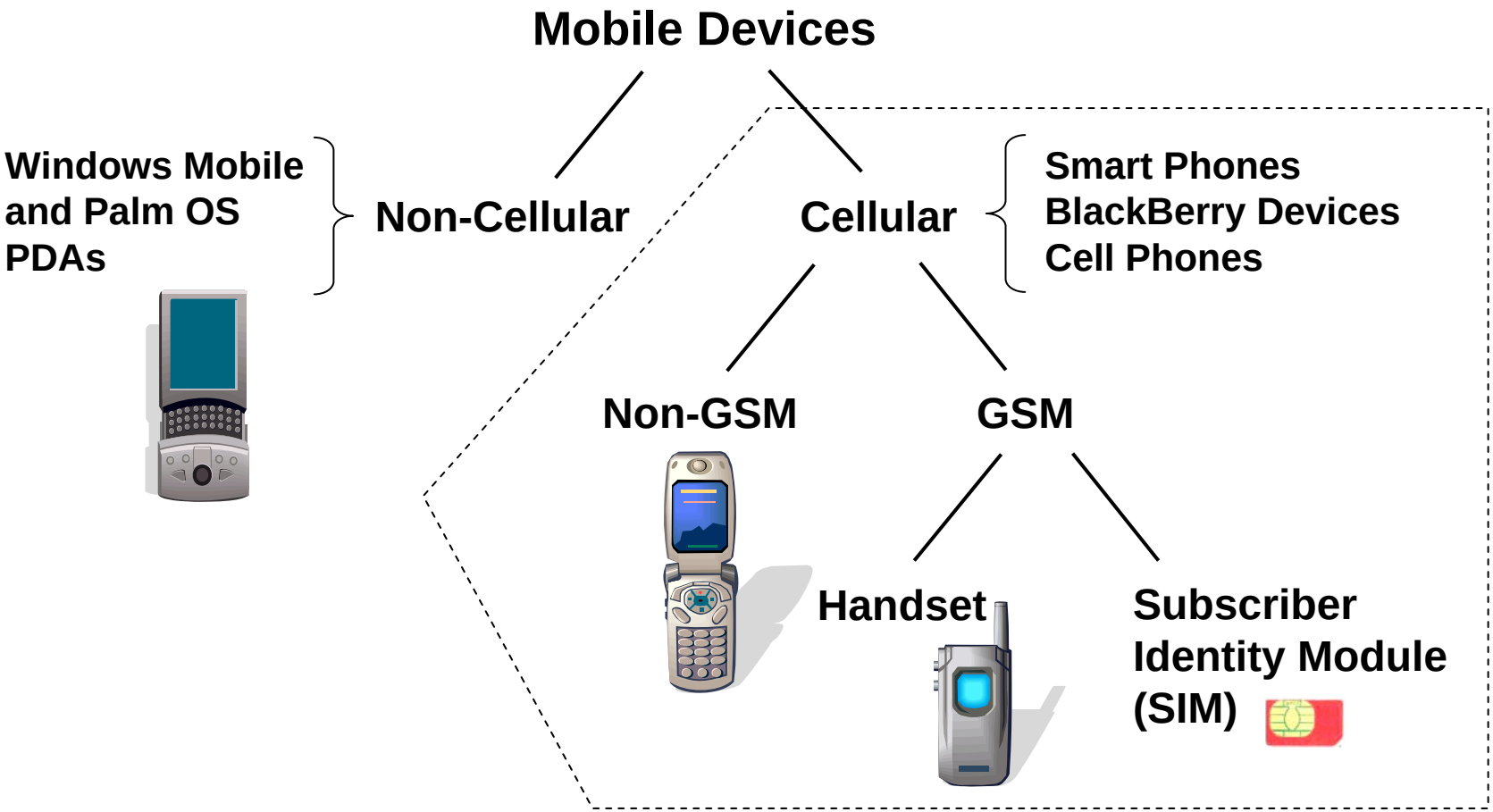
- AT&T rolled out the first cellular network in 1977 for 2,000 people in Chicago, with phones the size and weight of a brick
- Approximately 2 billion mobile phones are in the world today – 2 times the number of personal computers
- 1.1 billion handsets were sold in 2007
- Gartner estimates that about 1.9 trillion text messages were sent in 2007 and 2008 predictions reach the 2.3 trillion mark.



Footnotes

- A considerable number of software tools exist, but the range of devices addressed is often by:
  - a manufacturer's product line (e.g., Acquisition support for Nokia devices only)
  - an operating system family (e.g., Palm OS devices, Symbian devices)
  - a specific type of acquisition protocol (e.g., CDMA phones)
- The means of acquiring data may also range from connections via cable only to include infrared and Bluetooth alternatives
- Facilities for examination or reporting may not be provided, requiring other means to perform those tasks

Simplified Tool Classification



Device/SIM Architecture

- Internal Memory
  - Smart Phones
    - Flash ROM
      - OS
      - Pre-loaded applications
      - Safe-store folder
    - RAM
      - Program Memory
      - Object Store
  - Cell Phones
    - Flash
      - OS
      - User allocated space
- SIMs
  - Smart card that provides users with extended non-volatile storage
    - Processor
    - ROM
    - RAM
  - Essential element for GSM network authentication
  - Essential for GSM device functionality

Preservation

- **Inactive Device**
  - Leave off until in a protected laboratory setting
  - Seize all associated cables and media (i.e., SIMS, SD cards, CF cards)
- **Active Device**
  - Power it off
    - May trigger authentication mechanisms
    - May change the current state of the device
  - Faraday Bag
    - Not proven 100% effective
    - Must use a portable battery supply or a shielded cable charger
  - Acquire device on-site
- **Caveats**
  - Improperly shielded active devices may result in:
    - Overwritten data that is not recoverable
    - Updated LOCI data

Netherlands Forensic Institute
http://www.holmes.nl/MPF/FlowChartForensicMobilePhoneExamination.htm

Acquisition

- **SIM**
  - **PC/SC Reader acquires data objects defined by the GSM 11.11 standard**
- **Internal Memory**
  - **Physical**
    - **Physical acquisition implies a bit-by-bit copy of an entire physical store (e.g., a memory chip),**
    - **Advantages**
      - **Allows deleted files and any data remnants present to be examined, which otherwise would go unaccounted**
  - **Logical**
    - **Logical acquisition implies a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside on a logical store (e.g., a file system partition).**
    - **Advantages**
      - **System data structures are normally easier for a tool to extract and provide a more natural organization to understand and use during examination**

Evidence Sources

- Phonebook
- Calendar
- To do list

- Electronic mail
- Instant messages
- Web information

- Electronic documents
- Photos
- Videos
- Audio
- Graphics

- Subscriber identifiers
- Equipment identifiers
- Service Provider

- Last dialed numbers
- Phone number log

- Short text messages
- Enhanced messages
- Multimedia messages

- Last active location (voice and data)
- Other networks encountered

Tool Validation

- **CFTT – Computer Forensics Tool Testing Program provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results.**
- **Tool validation results issued by the CFTT project at NIST provide information necessary for:**
  - **Toolmakers to improve tools**
  - **Users to make informed choices about acquiring and using computer forensic tools**
  - **And for interested parties to understand the tools capabilities**
- **The CFTT project is further described at: http://www.cftt.nist.gov/**

Mobile Forensic - CFTT Documents

- **Mobile Device Imaging Specs**
  - **Requirements:** *GSM Mobile Device and Associated Media Tool Specification*
  - **Test Plan:** *GSM Mobile Device and Associated Media Tool Specification and Test Plan*
- **Test Setup Documents**
  - **Setup and Test Procedures:** *GSM Mobile Devices and Associated Media Tool Setup and Test Procedures*
- **Test Reports**
  - **Tool Test Reports: Results available later in the year**

http://www.cftt.nist.gov/mobile_devices.htm

Core Requirements

Internal Memory

- Device Recognition
  - Cable, Bluetooth, IrDA
- Non-Supported Devices
  - Error message
- Connectivity Errors
- Report Generation
  - GUI, Report
- Logical Acquisition
  - Tool supported data objects

SIM

- Media Recognition
  - PC/SC, proprietary reader
- Non-Supported SIMs
  - Error message
- Connectivity Errors
- PIN
- Report Generation
  - GUI, Report
- Logical Acquisition
  - Tool supported data objects

Optional Requirements

Internal Memory / SIM Acquisition

- Data Presentation
  - GUI, Report
- Case Data Protection
- Physical Acquisition
- Access Card Creation
- Log File Generation
- Foreign Language
- Remaining Number of PIN/PUK attempts
- Stand-alone Acquisition
- Hashing
  - Overall Case File, Individual Acquired Files

Core Assertions – Data Objects

SIM Data Objects

- Service Provider Name (SPN)
- Integrated Circuit Card Identifier (ICCID)
- International Mobile Subscriber Identity (IMSI)
- Mobile Subscriber International ISDN Number (MSISDN)
- Abbreviated Dialing Numbers (ADN)
- Last Dial Numbers (LDN)
- Short Message Service (SMS)
- Enhanced Message Service (EMS)
- Location Information (LOCI)
- General Packet Radio Service (GPRS) location

Internal Memory Data Objects

- International Mobile Equipment Identifier (IMEI)
- Personal Information Management (PIM) data:
  - Address book
  - Calendar entries
  - To-Do list
  - Memos
- Call Logs
- SMS text messages
- MMS messages
- File Storage: graphic, audio, video

Conclusions

- **Multiple tools are needed to cover the widest range of available mobile phones**
- **Understanding of proper seizure and preservation techniques are paramount**
- **Practice in mock examinations can help gain an in-depth understanding of a tool and subtleties of use, and also provides the opportunity to customize settings for later use**
- **Quality control and tool validation for Mobile Device Forensic tools is significant for proper data acquisition and reporting**

Sponsor Information

<u>Supporting Organizations</u>

Office of Law Enforcement and Standards (OLES)

National Institute of Justice (NIJ) &

Other Law Enforcement Organizations

Contact:

Susan Ballou

susan.ballou@nist.gov

Thank You!

Contact Information:

Rick Ayers

richard.ayers@nist.gov

- http://www.cftt.nist.gov/mobile_devices.htm
- http://csrc.nist.gov/mobiledevices/projects.html