Federal Law Enforcement Training Center

Cell Phone investigations

NAME
Senior Instructor
Technical Operations Division

Objective

Given an investigative scenario relating to the seizure of digital evidence, the officer will demonstrate the ability to seize, transport and store a cell phone in such a way as to preserve evidentiary integrity.

Homeland Security

“Handheld Devices”

Since the process of seizure of other handheld devices, such as PDA’s and Pagers, are similar to that of cell phones, this presentation also includes discussion of these related technologies.

Homeland Security

What is a ‘Handheld Device’

- An electronic device designed for a limited or specialized application.
- Including (or found in) Industrial Machines, Automobiles, Medical Equipment, Cameras, Household Appliances, Airplanes, Vending Machines, Toys,…
  - And the more obvious Cell Phones and PDA’s
- May be either ‘fixed capability’ or contain a ‘programmable interface’ with (usually) data dump capability

Homeland Security

Purpose of Seizure

- Trace Evidence Analysis
  - DNA, Prints, Other Types of Analysis
- Data Acquisition and Analysis

Homeland Security

A Look at Cell Phones

This course will concentrate on cell phones seizure.

But the principles can generally be applied to other handheld devices.

Homeland Security

Why Are We Interested?

Cell phones can provide any or all of the following…

- Contact Information
- Tasks/to-do lists
- Calendars and Schedules
- Calculation Results
  - When the cell phone is used as a calculator
- Received e-Mail
- E-Mail logs
  - Sending and Receiving
- Internet Pages
- Data From Attached Devices
  - PDA's MP3's, GPS Devices, etc.
- Audio Files
- Photographs
- Text Messages
- Text Logs
- Subscriber Information
  - Service Provider, ESN, etc.

Homeland Security

How Did We Get Here???

A (very) brief look on the history of cell phone technology including:

- **How we got here…**
- **Where we are…**
- **And where we are going**

Homeland Security

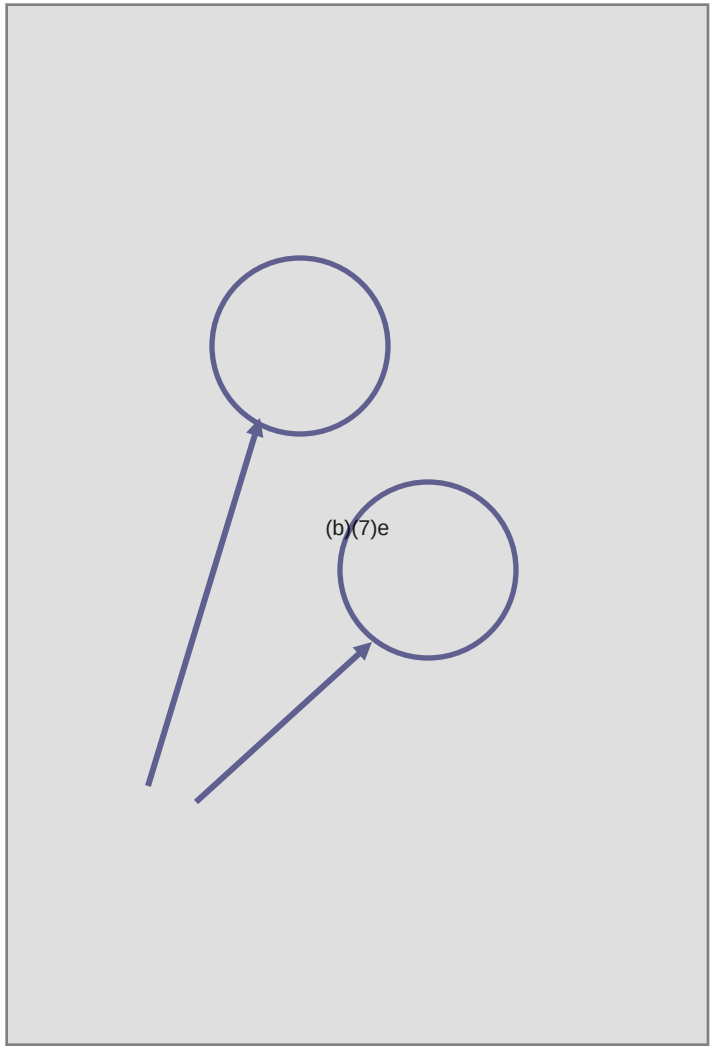
In the Old Days….

- Prior to 1983 (the birth of modern first generation cell technology), mobile communications required a powerful radio-receiver.
- High-powered transmitter was required
- Communications channels limited to 25 in a single geographic area.
- Devices were bulky and heavy.
- Transmission Relay towers were few and far between (or nonexistent).

Homeland Security

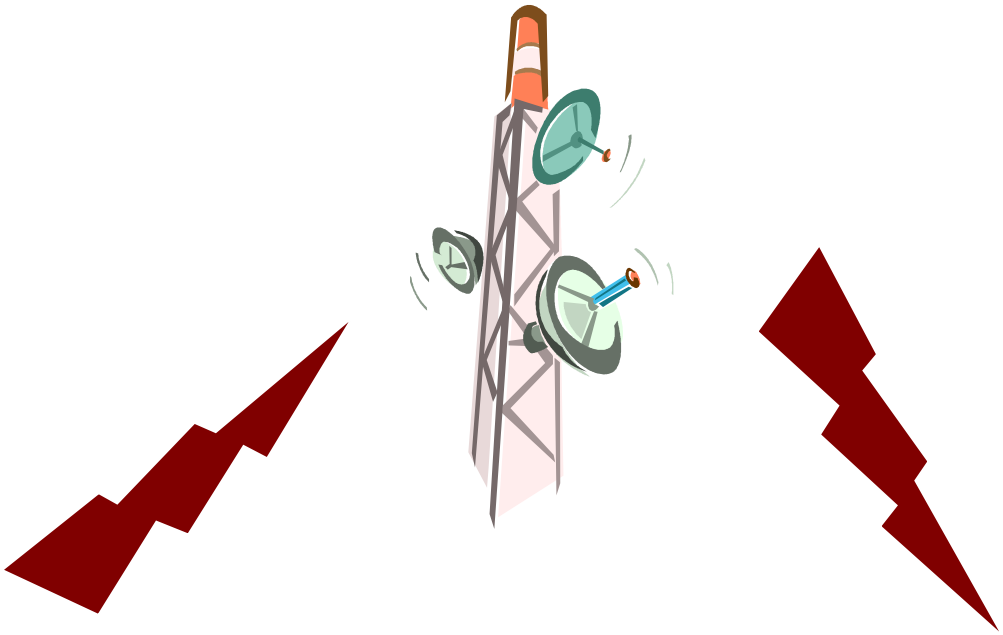
Cell Phones: The Basics

- Each Cell Carrier is provided (by FCC) 832 frequencies per geographic area.
  - Of these, 42 are used by the carrier for system control
- These frequencies are distributed via “cells”, each of which is about 10 square miles in area.
- Each cell is assigned 56 voice channels.
- When users move from cell to cell, frequencies change without noticeable interruption.



Homeland Security

How it Works

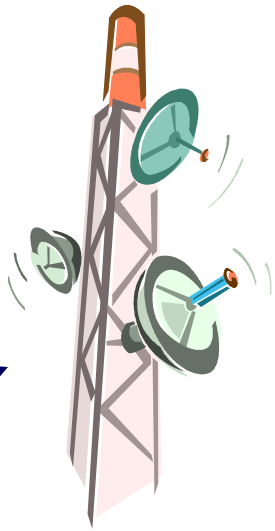


MTSO
(Mobile Telephone Switching Office)

PSTN
(Public Switched Telephone Network)

Homeland Security

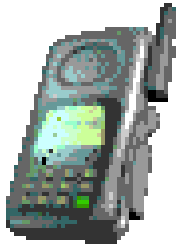
Placing a Call



Synchronizes signal and forwards it to MTSO

912-267-2314

SEND



MTSO processes cell-to-cell, Internet, e-mail

For Land-Based communication, forwards signal to phone company (PTSN)

Homeland Security

Cell Phones: The Basics

- By using multiplex technology these 56 assigned channels can provide substantially more simultaneous conversations.
- For example, TDMA technology can interlace three conversations on a single channel.
- CDMA can typically interlace 10 or more communications on a single channel.

Cell Phones: The Evolution

- In 1983, the first digital cell technology was introduced.
  - Voice Only
- Cell phones were very basic communications devices
  - But still are frequently encountered
  - May contain call logs and contact lists

Homeland Security

Cell Phones: The Evolution

Current Cell Technology

- **TDMA**
  - **Voice Only. Oldest digital technology.**
- **CDMA**
  - **Voice as well as other data (photos, email, etc.)**
- **GSM (Global Systems Mobile for Communications)**
  - **The standard in 168 different countries**
  - **Allows for cell communications when you travel to (e.g.) Botswana**
  - **Identifying feature: It requires a SIM memory card**

Homeland Security

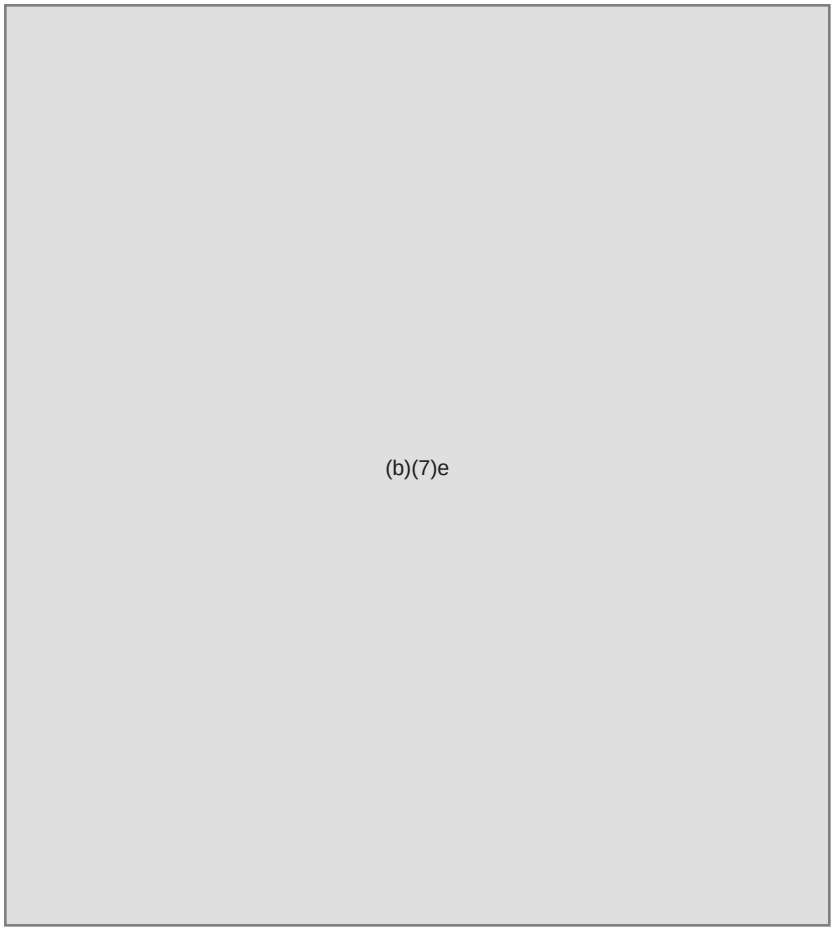
Cell Phones: The Evolution

- AT&T Wireless and Cingular recently switched to GSM.
- CDMA and GSM are now the only major technologies in the U.S.
- The GSM-required (removable) SIM Card contains:
  - Cell Subscriber Information
  - Everything else (photos, music, email, web pages, etc.)
- When upgrading a GSM phone, just change memory cards!

Homeland Security

Cell Phones: Service Providers

- **Alltel:**
- **AT&T:**
- **Cingular:**
- **Nextel:**
- **Sprint:**
- **T-Mobile:**
- **U.S.Cellular:**
- **Verizon:**



Homeland Security

Cell Phones: What's Next

The staggering implications of '4G' cell service is only two or three years away.

- **Higher frequencies and broader bandwidth**
- **Will enable live (real time) video transfer**
- **Will allow your iMAC to be your cell phone**
- **Your cell phone can subscribe to XM-Radio**
- **Your Blackberry can play real-time movies**
- **Integrated cell and Internet and email technologies**
- **'Killer' application waiting to be born**

Homeland Security

Cell Phones: Important Codes

- **ESN: Electronic Serial Number**
  - **A unique 32-bit number programmed into the phone at manufacture**
- **MIN: Mobile Identification Number**
  - **Your assigned 10-digit phone number**
- **SID: System Identification Code (or ‘Data’)**
  - **A unique 5-digit code assigned to your mobile provider**

(b)(7)e

Homeland Security

Cell Phone Manufacturers

- Nokia
- Motorola
- LG (Life's Good!)
- Siemens Mobile
- Samsung
- Sony Ericsson

Homeland Security

Cell Phone Trivia

- 42% of cell phone users say they will upgrade to a new phone within the next year.
- 11% say they will buy a new brand.
- In 2005, 26% of all cell phone users switched service providers.
- 60% of all cell phone calls are made outdoors
  - Of which 62% are made from vehicles and 36% are made while walking or standing
- 20% of cell phone users don't know their brand name (47% are Nokias!)

Homeland Security

Cell Phone Manufacturers

Nokia

Homeland Security

Cell Phone Manufacturers

Motorola

Homeland Security

Cell Phone Manufacturers

Siemens Mobile





Homeland Security

Cell Phone Manufacturers

Samsung

Homeland Security

Cell Phone Manufacturers

LG (“Life’s Good!”)

Homeland Security

Cell Phone Manufacturers

Sony Ericsson

Homeland Security

Cell Phone Seizure

The Four Rules of Cell Phone Investigations

Homeland Security

Cell Phone Seizure

Rule 1:

(b)(7)e

Homeland Security

Page 30 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)e

Cell Phone Seizure

(b)(7)e

Homeland Security

Cell Phone Seizure

(b)(7)e

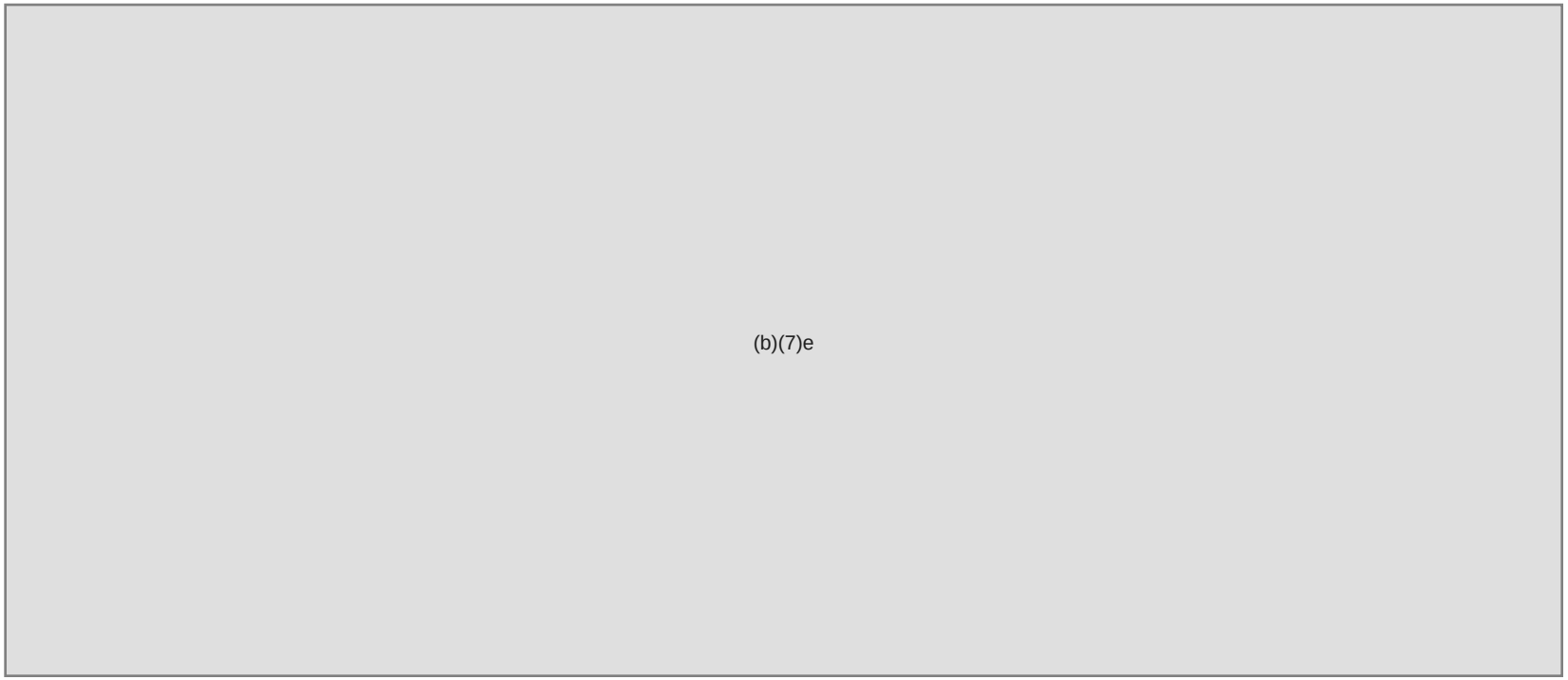
Homeland Security

Cell Phone Seizure

(b)(7)e

Homeland Security

Cell Phone Seizure



Homeland Security

Cell Phone Seizure

Rule 2:

(b)(7)e

Homeland Security

Cell Phone Seizure

- (b)(7)e

Homeland Security

Cell Phone Seizure

Cell phone accessories include…

- Bluetooth devices
- Covers
- Earpieces
- Batteries
- Mikes
- Cameras
- Antennas
- Cables
- Chargers
- Transport devices
- Adapters
- Speakers

Homeland Security

Cell Phone Seizure

Rule 4:

(b)(7)e

Homeland Security

Cell Phone Seizure

At the Site

(b)(7)e

Homeland Security

Cell Phone Seizure

At the Site

(b)(7)e

Homeland Security

(b)(7)e

Seizing Pagers

(b)(7)e

Homeland Security

(b)(7)e

Computer v. Handheld Acquisition

COMPUTER	*HANDHELD*
(b)(7)e	

Homeland Security

Cell Phone Analysis

- **Cell phone acquisition and analysis is fairly unsophisticated.**
- **You need a Hardware Kit.**
  - **Contains cables and interfaces for every known cell phone.**
- **And a Software Kit**
  - **A computer program that, when run, hoovers the data from the cell phone, assimilates and sorts it, and gives it back in the form of printed (and saved) reports.**

Homeland Security

Cell Phone Analysis

(b)(7)e

Homeland Security

Legal Considerations

- **Seizure of cell phones and accessories should be included as part of any search warrant.**
- **Subsequent analysis of cell phone data should be handled carefully – and legally.**

Did you hear about the new sushi bar that caters exclusively to lawyers? It's called 'SoSumi'.

Homeland Security

Legal Considerations

At least two additional legal statutes should be considered when dealing with cell phone evidence.

(b)(7)e

Homeland Security

Legal Considerations

Title III is relevant because:

- Cell phones are devices for receiving ‘aural’ (or voice) communications.
- Part of all cell communications travels through ‘wires’.

Homeland Security

Legal Considerations

ECPA is relevant because:

- Cell phone service providers retain certain information related to subscribers, their accounts and activities.
- The acquisition of this data is largely regulated by ECPA.

Homeland Security

Legal Considerations

ALWAYS…

…get legal counsel from your prosecutor our agency counsel prior to any evidence analysis of a cell phone, PDA, or other handheld device!

That way, you'll have somebody to blame is something goes wrong!

Homeland Security

Summary and Conclusion

- Cell phones and other handheld devices are a critical part of investigative evidence-gathering.
- Always protect the integrity of the evidence
- When processing cell phone evidence, remember the four rules of cell phone evidence.
- Every search warrant should include stipulations for seizing cells and PDA's.

Homeland Security

Federal Law Enforcement Training Center

Name

Senior Instructor

Technical Operations Division

Digital Forensics Branch

(b)(6)

first.last@dhs.gov