

## Overview

- PDA (cell phones)
- Email

[Class discussion - FB](#)

[Cell Phone Forensic Expert](#)  
missing students

[Spouse – VM](#)

[Duke case](#)

Laci Peterson case

[Video evidence against police or suspect?](#)

[The Hofstra case](#)

[What your Cell Phone knows about you](#)



## What Is Stored on your PDAs

- Calls
- Texts
- Email
- IM (logs)
- Web – bookmark
- Pictures (sent and received)
- Calendars
- Applications (potential problem)
- Contacts
- Music
- Audio/ video
  
- Very personal information
  
- Primary damage
- Secondary damage – often even more damaging than primary

## The Popularity of PDAs

- Computers are ubiquitous – touches almost all aspects of our daily lives
- BUT PDAs (cell phones) are even more so – including in rural areas
  - Why?
- Yet most people don't take enough precaution to safeguard their PDAs
- “PDAS contain a great amount of information that essentially is a subjective picture of our habits, our friends, our interests and activities, and now some even have location tracking”
- “Most cell phone owners think simply removing a phone's SIM card removes personal information, but the phone's internal memory, even communication exchanged between the phone and its server, remain”
- Europe
- Pictures taken – with geolocate
  - pros and cons

## Why it is hard to carry out forensic analysis on PDAs

- But not all cell phones respond to modem-style commands and some cell phone developers are often loath to share their proprietary technology.
- Nokia phones are particularly hard to crack. In the U.S. alone there are over 2,000 models of phones. Constant state of catch-up — a company rolls out new models every three to six months; that's how they make money (along with applications).
  - What is the trouble of applications (PDAs)
- The Holy Grail for the cell phone code breakers is to develop a forensics tool to break into any cell phone
- Read more:  
<http://www.time.com/time/health/article/0,8599,1653267,00.html#ixzz0XfXF BxVG>

## Smartphone Security / Risks

- While there is the problem of many mobile-phone SIM cards contain contacts and texts deleted from years ago, it is actually the vastly improved **data and storage capacity** of the new generation of smartphones that presents the most potent risk to their owners.
  - Is this really a big problem, or are we making too big of a deal
- It is not what is recoverable from the phone that is valuable but what can be further discovered online, by further using this easily accessible information.
- Even though most smartphones can be locked by the carrier after being stolen or lost, technology now exists to make a physical clone of a phone in very quickly – before the owner is aware of the loss
- "There are cheap analysis tools on the market that might cost only a few hundred dollars that would allow you to do a physical dump of every piece of data on the phone before it gets locked" (forensic analyst – see link)

## Smartphone Forensics

- Geospatial mapping capabilities now becoming commonplace in smartphones - photos often also contain the GPS co-ordinates of the phone as well as date and time stamp
- Forensic analysis can be used to prove the location at a point in time of people in the photo (what is the problem with this from a user perspective?)
- Mobile phone forensics comprise an important part of crime detection and corporate security – but are also playing a role for private detectives investigating marital or work disputes (when phone towers are accessed – and what angle, how far, how long ...)

## SIM Cards

- Subscriber Identity Module (SIM) cards – SIM and mobile equipment (cell phone or PDA)
  - easily accessible by anyone (!)
  - switching SIM cards is a common international practice
  
- The SIM card is necessary for the ME to work and serve the following (amongst others):
  - Identified the subscriber to the network stores personal info
  - Stores address books and messages
  - Stores service-related information
  
- Forensic specialists must check and collect at least the following:
  - the internal memory
  - the SIM card
  - any additional removable or external memory cards
  - the system server
  - all and any cables – because ...

## Mobile Forensic Tools

- Paraben (Seizure Toolkit)
  - Includes assorted cables (that interface with different makes of PDAs) , a SIM card reader
- BitPim – views data on several makes of phone – but is used in conjunction with forensic tools
- MOBILedit
  - Built-in write blocker
  - Connects to phone directly via Bluetooth, IR or cable
  - Very user-friendly
- SIMCon
  - Images files (stored numbers and text messages)

Most mobile forensic tools's features include:

- Reads files on SIM cards
- Analyses file content, including text messages and stored numbers
- Recovers deleted text messages
- Manages PIN codes
- Generates reports that can be used as evidence
- Archives files with MD5 and SHA1 hash values (why is this necessary?)
- Exports data to files that can be used in spreadsheet programs
- Supports international character sets

## Email

- Email protocols
  - SMTP
    - SMTP servers (sent and received)
  - POP3
    - POP3 servers (access info)
  
- Examining Email Headers
  - The header contains unique identifying numbers – IP, date, time, heading, cc
  
  - Phishing emails from Nigeria
    - Yahoo, gmail, Outlook
  - Examples of doctoring forwarded email
    - See forwarded message below
  - Examples of exchanging email headers – spoofing email (2001 Suni Munshani v. Signal LakeVenture)
    - Using one email for another

## Specialized Email Forensic Tools

- FINALeMAIL
  - Outlook, Eudora
  
- Sawmill-Group Wise
  - Log Analysis
  
- DBXtract
  - Outlook
  
- Paraben Email Examiner
  - Several email formats
  
- AccessData FTK
  - Outlook
  
- Ontrack Easy Recovery EmailRepair for Outlook
- R-Tools R-Mail for Outlook
- OfficeRecovery's MailRecovery