Basic Cell Phone and PDA Forensics

Matt Churchill
Douglas County Sheriff's Office

NebraskaCERT Conference 2007

Agenda

- Who am I?
- Considerations in handheld forensics
- What should I try to recover?
- Hardware tools
- Software tools
- Building your toolkit
- What's next?
- Resources

Who am I?

- 10 years LE experience
- Three and half years of computer forensics experience
- CFCE, CCE certified
- IACIS, ISFCE, HTCIA member

Forensic Considerations

- GSM, CDMA, TDMA, IDEN
- 1st, 2nd, 3rd Generation
- SIM Card – Yes or No
- Additional memory sources
- Recoverable items may depend on phone model, service, subscription types

Forensic Considerations

- Handheld seizures
  - Leave it on or turn it off?
    - If left on, must isolate from network
      - » Battery will drain more quickly as phone searches for network
      - » Could the PDA or phone run any destructive programs if left on?
    - If turned off, you risk the phone/PDA being password protected

Forensic Considerations

- Take charger and data cable if available
- Look for phone documentation
- Remove the battery for info?
  - IMEI can be obtained by keying in *#06#

What to Report

- Make, Model, Color, Condition
- IMEI, SIM card number
- Hardware/Software Used
- Data recovered

What to Recover

- Depends on Phone/PDA model
- In addition to identifying characteristics…
  - Call Logs, Phonebook
  - Calendar
  - Text, Audio, Video
  - Messages sent/received
  - Internet cache, settings
  - Hex dump, filesystem

Hardware Tools

- Universal Battery Charger
- Faraday bags/cages
  - Aluminum foil, arson cans
- SIM Card Readers
  - Forensic Card Reader
  - SIMIS
  - Many cable kits come with SIM Card reader

Hardware Tools

- Cable Kits
  - DataPilot
  - Paraben
  - www.cellphoneshop.net, single cables
  - Other hardware contains their own cables…

Hardware Tools

- Cellebrite Universial Memory Exchanger, UME-36Pro, $1300
  - Forensic version is coming…
  - Includes Cables
  - Excellent customer support
  - Collects internal memory, SIM card content, phonebooks, pictures, videos, ring-tones, and SMS.

Hardware Tools

- Logicube CellDek, $20k
  - Self contained unit w/cables
  - Acquires data and produces report
  - Biggest complaint is price, proprietary nature

Hardware Tools

- Project-a-Phone, $400
  - USB camera used to capture manual analysis

Software

- Phone Manufacturer Software
  - Not forensically sound
  - Limited capabilities
  - Might be your only choice
- Examples
  - Nokia PC suites
  - Siemens PC software and drivers
  - Motorola Data Suite
  - Samsung Mobile Phone Support

Software

- Paraben's Device Seizure, $895
  - Combined PDA and Cell Seizure into Device Seizure
  - Long considered as the "standard" product
  - Logical and filesystem acquisition

Software

- BitPim
  - Used for CDMA phones, LG, Motorola, Samsung, Sanyo
  - Designed to manipulate the data on the phone, including filesystem
  - Now includes write blocking option

Software

- MOBILedit!, $400
  - Primarily GSM phones
  - 367 supported phones in latest version, 2.3.0.14
- Oxygen Forensic Suite, $750
  - Support for Nokia, Sony Ericsson, Symbian OS Smart Phones
  - More than 200 devices supported

Software

- DataPilot SecureView, $645
  - Over 650 supported devices
  - Hardware key allows multiple installations
  - 2 years free updates & cables

Building Your Toolkit

- Must have several software programs available
- Might get different results with different tools
- Drivers may conflict between software programs
- Consider installing each software suite in it’s own VM on dedicated cell phone forensic machine

What's Next?

- Hex Dumps
  - Physical acquisition of phone memory
  - Need "flasher" or "twister" device
  - New software available to analyze hex dump or "flash file" and create report
  - Pandora's Box for Nokia phones
  - Cell Phone Analyzer for Nokia, Sony Ericsson, Samsung, limited Blackberry and Motorola support

Resources / Acknowledgements

- Papers
  - http://www.techsec.com/TF-2006-PDF/TF-200
  - http://csrc.nist.gov/publications/nistir/nistir-725
  - http://csrc.nist.gov/publications/nistir/nistir-738
  - http://www.holmes.nl/MPF/Principles.doc

Resources / Acknowledgements

- Papers
  - http://csrc.nist.gov/publications/nistpubs/800-1
  - http://www.search.org/files/pdf/CellphoneInves
  - IACIS 2007 Basic Conference Student Manual

Resources / Acknowledgements

- Websites
  - http://www.ssddforensics.com/
  - www.e-evidence.info/cellular.html
  - www.mobile-examiner.com
  - http://mobileforensics.wordpress.com/
  - http://trewmte.blogspot.com/
  - http://www.mobileforensicscentral.com/mfc/
  - http://tech.groups.yahoo.com/group/phoneforensics/
  - http://mobileforensicstraining.com/