Outline

1. NIST
   1. Background
      - Hardware Classification: Basic, Advanced, High End
      - Identity Module: SIM (Identification and Storage)
      - Removable Media: SD Memory Stick
   2. Tools: NIST 7100
      - PDA Secure
      - EnCase
      - pdd
      - pilot-link
      - POSE
      - dd
   3. Background
      - Hardware Classification: Basic, Advanced, High End
      - Identity Module: SIM (Identification and Storage)
      - Removable Media: SD Memory Stick
   4. Tools: NIST 7100
      - PDA Secure, EnCase
      - Phone
      - SIM
   5. Background
      - Hardware Classification: Basic, Advanced, High End
      - Identity Module: SIM (Identification and Storage)
      - Removable Media: SD Memory Stick
   6. Tools: NIST 7100
      - PDA Secure, EnCase
      - Phone
      - SIM

Extras

NIST - NISTIR 7100

1. Background
   - Hardware Classification: Low End, Mobile, High End
   - Removable Media: CF, Microdrive, MMC, SD, Memory Stick
2. Tools: PDA Secure
   - Devices: Palm OS and Pocket PC
   - Features: Acquisition, Search, Graphics, Bookmarking, Report Generation, Password Cracking
3. Tools: EnCase
   - Devices: Palm OS and Linux
   - Features: Acquisition, Search, Scripts, Graphics, Filters, Report Generation
4. Tool: pdd
   - Devices: Palm OS
   - Features: Acquisition
5. Tool: pilot-link
   - Devices: Palm OS
   - Features: Acquisition
6. Tool: POSE
   - Devices: Palm OS
   - Features: Emulator
7. Tool: dd
   - Devices: Linux
   - Features: Acquisition
   - Note: Possible to dump to remote machine using netcat

NIST - NISTIR 7250

1. Background
   - Hardware Classification: Basic, Advanced, High End
   - Identity Module: SIM (Identification and Storage)
   - Removable Media: SD Memory Stick
2. Tools: NIST 7100
   - PDA Secure, EnCase
   - Phone
   - SIM
3. Tools: Phone
   - Cell Seizure, XRY, Oxygen PM, MobiEdit Forensic, BiPIM, TULP 2G
4. Tools: SIM
   - Cell Seizure, TULP 2G, XRY, MobiEdit Forensic, SIMs, Forensic SIM, Forensic Card
   - Devices
   - Features
   - Model Name: Contacts, Calls, Calendar, SMS, Pictures, Audio, Notes, Task, SIM, Network Information, Video, Graphics, etc.
Background

- Cellular Networks: CDMA, GSM, TDMA, IDEN, D-AMPS
- Hardware Classification: Basic, Advanced, Smart
- Identity Module, NIST 7100 + USIM (Authentication and Storage)
- Removable Media: NIST 7250 + micro formats

Tools: NIST 7100 + 7250

- Forensic Card Reader, ForensicSIM, SIMCon, SIMIS, BitPIM, Oxygen PM, PDA Seizure, Pilot-link, Cell Seizure, GSM .XRY, MOBILedit!, TULP 2G

Tools: SIM

- NIST USIMdetective, Oxygen PM for Symbian, CellDEK, PhoneBase, SecureView

Device: ICID, ADN, LND, LOCI, EMS

Outline

1 NIST
2 Law
3 Memory
4 Extras

NIST guides are for the most part outdated
Provide detailed test case scenarios
Documents outline each tools capabilities and performance
Cover mobile forensics in the Personal Digital Assistant (PDA) era [Palm OS, Symbian, Windows CE, SIM]

Introduction

Abstract

- Rapid growth and production of mobile devices in our society
  - 2008 worldwide cellular subscriber base (4 billion)
  - Mobile devices outsell PCs (3 to 1)
- Mobile devices are small, functional, portable data carriers
- Increase in potential admissible digital evidence in civil or criminal cases [12]
Introduction

Goals
1. Types of digital evidence
2. Differences between mobile and computer forensics
3. Weaknesses of mobile forensic toolkits and procedures
4. Impact emerging technologies have on digital evidence

Types

- Mobile Office
  - Word processor, spreadsheet, database, PDFs
- Short Message Service (SMS) Messages
  - India 2008, 1.5 billion per week
- Enhanced Message Service (EMS) Messages
- Multimedia Message Service (MMS) Messages
  - India 2008, 10 million per week
  - 30% growth per year
- "Push" IMAP / "Pull" POP Email
- Internet Downloads (Web, Music, Videos, Ringtones)
- Instant Message Service (IM) Messages
- Wireless Application Protocol (WAP) Transactions
  - E-wallet, stock trading, mobile banking

Differences - Reproducibility

Dead (Offline) Analysis
1. Device is OFF
2. Image of Hard Disk (HD)
3. Hash(Image HD) = Hash(HD)
4. Use trusted OS and forensic applications to evaluate hard disk image

Problem
- Hash(Image HD) != Hash(HD)
- Why: The device clock constantly changes, and is actively updating information in memory. Even when the device is powered off, it is impossible to obtain a bit-wise copy of the entire contents of memory because the hash value will be different every time the function is applied.

Differences - Connectivity

Live (Online) Analysis
1. Device is ON physically
2. Device is ON logically
3. Use forensic applications to evaluate device

Problem
- As of 2008, live analysis of mobile devices is unheard of
**Differences - OS and File Systems**

- **OS and File Systems**
  - Wide variety of operating and file systems
  - Proprietary closed source
  - Many manufacturers

- **Problems**
  - Development and testing of forensic tools becomes onus task
  - Developers are reluctant to release the inner workings citing them as trade secret
  - Extremely short release cycles for operating system

**Differences - Hardware**

- **Hardware**
  - Typical: microprocessor; main board; Read Only Memory (ROM); Random Access Memory (RAM); radio or antenna; Digital Signal Processor (DSP); display; microphone; speaker; input device; battery
  - Extra: digital camera; Global Positioning System (GPS); wireless network; hard disk

- **Problems**
  - Manufacturers and carriers highly customize OS
  - ROM updates are OS and hardware specific
  - Proprietary hardware is not supported by forensic tools
  - Cable types for power and communication vary in shape, size, and specs

**Outline**

1. **NIST**
2. **Law**
3. **Introduction**
4. **Types**
5. **Differences**
6. **Weaknesses**
7. **Impact**
8. **Summary**

**Weaknesses - Definitions**

- **Scientific Working Group on Digital Evidence (SWGDE)**
  - Digital evidence is information of probative value that is stored or transmitted in binary form

- **Australian Standards HB171 - Guidelines for the Management of IT Evidence**
  - IT Evidence is any information, whether subject to human intervention or otherwise, that has been extracted from a computer. IT evidence must be in a human readable form or able to be interpreted by persons who are skilled in the representation of such information with the assistance of a computer program

- **Information Technology Act 2000**
  - Does not include information about mobile device evidence

- **UK Association of Chief Police Officers - Good Practice Guide for Computer based Electronic Evidence**
  - The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to

- **Compliance Problems**
  - 1. is not possible with mobile devices because of the hash problem discussed earlier
  - 2. requires a specialist to have expert knowledge of the hardware, software, and tools used to acquire evidence from the device
The general rules of evidence should be applied to all digital evidence.

Upon seizing digital evidence, actions taken should not change the evidence.

When it is necessary for a person to access original digital evidence, that person should be suitably trained for the purpose.

All activity relating to the evidence, access, storage or transfer of digital evidence must be fully documented, preserved, and available for review.

An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.

Compliance Problems

- As seen before, 2 is not possible with mobile devices because of the hash problem discussed earlier. In addition, the methods used by the tools are not forensically sound or verifiable.

Impact - Emerging Technology

- Processor
  System on Chip (SoC): contains unique instructions with built-in memory

- Battery
  Newer features that consume additional power will drain batteries faster, which can lead to loss of data

- Memory and Storage
  Require auditing trail for swappable external storage

Summary

MFL3G: Mobile Forensics Library

- Thesis for Mr. Syed Rizwan Ahmed, "MFL3G: Mobile Forensics Library for digital analysis and reporting of mobile devices for collecting digital evidence" [1]
- Google Scholar Search Result

- No documentation, source code, links, citations, and references are currently available for the thesis document or proposed tool

Resolve conflicts and expand in digital evidence definitions
Create standardized digital evidence policy, guidelines, and methodologies
Require freer flow of information about OS, FS, and Forensic Tools
Live memory forensics of mobile phones

School of Computing, National University of Singapore
Crypto. and Security Dept., Institute for Infocomm Research
1 Fusionopolis Way, 21-01, Connexis, Singapore 138632

Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Chang

Overview

Problems

1. "Pulling the Plug" may result in loss of important evidence
2. As storage media increases so does the processing time
3. Encryption and other obfuscation can hinder analysis
4. Evidence such as application, browsing, and instant messaging data is not stored on disk

Goals

1. Automated system that performs live memory analysis on Android phones
2. Investigate dynamic behavior of volatile memory
3. Recover evidence real-time from communication based applications

Overview - History

<table>
<thead>
<tr>
<th>Year</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>Willassen</td>
<td>Proposed extraction by desoldering memory chip and reading from programmer</td>
</tr>
<tr>
<td>2006</td>
<td>Casadei</td>
<td>SIM-brush tool (Linux and Windows)</td>
</tr>
<tr>
<td>2007</td>
<td>Kim</td>
<td>Tool to acquire data from Korean CDMA flash memory</td>
</tr>
<tr>
<td>2007</td>
<td>Al-Zarouni</td>
<td>Study of mobile phone flasher devices</td>
</tr>
<tr>
<td>2007</td>
<td>Oliver</td>
<td>Tool to acquire active files from Symbian OSv7</td>
</tr>
<tr>
<td>2008</td>
<td>Jansen</td>
<td>Baseline tool to populate SIM with test data</td>
</tr>
<tr>
<td>2009</td>
<td>Gaffaney</td>
<td>Evaluate iOS tools</td>
</tr>
<tr>
<td>2010</td>
<td>Husain</td>
<td>Analysis of iOS IM clients</td>
</tr>
<tr>
<td>Model</td>
<td>System Model</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>- MSG and Monkey</td>
<td>- Message Script Generator (MSG)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Randomly generates test message and monkey script</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- UI/Application Exerciser Monkey (Monkey)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Part of Android software stack</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Use to perform pseudo-random actions on phone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Can perform deterministic actions through Android Debug Bridge (ADB)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Memory Acquisition Tool (memgrab)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Process memory management is handled by the Linux 2.6 kernel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Anonymous shared memory is handled by the ashmem driver instead of the Linux kernel IPC module</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Low Memory Killer driver replaces the standard Out-of-Memory Killer module</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Relies on /proc/pid/maps (addresses) and /proc/pid/mem (memory)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Performs Process Trace (ptrace) system call (traces by controlling exec)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Memory Dump Analyser (MDA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Graphs from live memory forensics of mobile phones, Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Change</td>
<td></td>
</tr>
</tbody>
</table>

**Outline**

1. **NIST**
2. **Law**
   - Introduction
   - Types
   - Differences
   - Weaknesses
   - Impact
   - Summary
3. **Memory**
   - Overview
   - Model
   - Experiments
   - Conclusions
4. **Extras**
To prevent dumping of irrelevant memory regions they conducted an experiment to identify the region of memory where messages appear. In the experiment the PC and phone sent and received 15 messages each. For each entry in /proc/pid/maps the corresponding memory dump was searched.

**Results**

Messages were consistently found in the shared memory region. Heap and stack sections contain database initializations and chat session credentials. Heap and stack data is also frequently found in the cached data section.

**Cached Data Examination**

- **Purpose:** Determine what information is available in the cached section
- **Cached location:** /data/data/com.android.browser/databases
- Found: 3 SQLite databases: browser.db, webviewCache.db, and webview.db
  - browser.db contained bookmarks, URLs, and keywords from search history
  - webviewCache.db contained images, javascript, and cascading style sheets
  - webview.db contained formdata, httpauth, cookies, formurl, and password tables

**Results**

Chat messages were not available from the cached data section.

**Realistic Parameters**

- **Interval between Keypresses**
  - QWERTY keyboard measures 6.8cm from P to Q
  - Novice user can type average of 9.9 wpm
  - Experienced user can type average of 21.1 wpm
  - Assuming 5 characters per word
  - Worst case parameter and Normal Distribution user can type average of 24.1 wpm
  - Average delay between two keypresses is 500 ms

- **Character Set**
  - Printable characters (appear on phone QWERTY keyboard)
  - Only allow characters that require single keypress
  - Require: message length = number of keys pressed

- **Message Length**
  - Consider 3 different message lengths: 75, 150, 225
  - Require: the final key press to be the ENTER key
  - 75 - One meaningful sentence (15 words x 5 per word)
  - 150 - Short message (SMS - 160 vs Tweet - 140)
  - 225 - Two to three meaningful sentences

- **No-wait Scenario Interval**
  - (key) x (length - 1)

- **Wait Scenario Interval**
  - (2 x key) x (length - 1)

**Note**

Even though the message length is dependent on factors like the topic and chatting style, these are more complex to define and out of the scope of the experiment.
In a more realistic scenario where the parties take turns sending messages, as well as send messages back to back the recovery rate is more than acceptable and captures enough detailed information for further forensic analysis.