CS 6V81-05

Advanced Digital Forensics and Data Reverse Engineering - Mobile Forensics

Donald Talkington
dst071000@utdallas.edu

Department of Computer Science
The University of Texas at Dallas

September 30th, 2011

Outline

Outline

NIST

Aug 2004 - NISTIR 7100 PDA Forensic Tools: An Overview and Analysis

Technology Administration, U.S. Dept. of Commerce

Rick Ayers and Wayne Jansen

Oct 2005 - NISTIR 7250 Cell Phone Forensic Tools: An Overview and Analysis

Technology Administration, U.S. Dept. of Commerce

Rick Ayers, Wayne Jansen, Nicolas Cilleros, and Ronan Daniellou

May 2007 - SP800-101 Guidelines on Cell Phone Forensics

Technology Administration, U.S. Dept. of Commerce

Rick Ayers and Wayne Jansen

NIST - NISTIR 7100

1. Background
   - Hardware Classification: Low End, Middle, High End
   - Removable Media: CF, Microdrive, MMC, SD, Memory Stick
2. Tool: PDA Seizure
   - Devices: Palm OS and Pocket PC
   - Features: Acquisition, Search, Graphics, Bookmarking, Report Generation, Password Cracking
3. Tool: 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 (Authentication and Storage)
   - Removable Media: NIST 7100
2. Tools: NIST 7100
   - PDA Seizure, pilot-link
3. Tools: Phone
   - Cell Seizure, GSM .XRY, Oxygen PM, MOBILedit! Forensic, BitPIM, TULP 2G
4. Tools: SIM
   - Cell Seizure, TULP 2G, GSM .XRY, MOBILedit! Forensic, SIMIS, Forensic SIM, Forensic Card Reader, SIMCon
   - Device: Name, Manufacturer, Model, Serial (IMEI), Subscriber ID (IMSI), code, and device clock
   - Store: Contacts, Calls, Calendar, SMS, Pictures, Audio, Notes, Tasks, MMS, Network Information, Video, Graphics, et. al.

NIST - SP800-101

1. Background
   - Cellular Networks: CDMA, GSM, TDMA, IDEN, D-AMPS
   - Hardware Classification: Basic, Advanced, Smart
   - Identity Module: NIST 7250 + USIM (Authentication and Storage)
   - Removable Media: NIST 7250 + micro formats
2. Tools: NIST 7100 + 7250
   - Forensic Card Reader, ForensicSIM, SIMCon, SIMIS, BitPIM, Oxygen PM, PDA Seizure, Pilot-link, Cell Seizure, GSM .XRY, MOBILedit!, TULP 2G
3. Tools: SIM
   - USIMdetective, Oxygen PM for Symbian, CellDEK, PhoneBase, SecureView
   - Device: Integrated Circuit Card ID (ICCID), Abbreviated Dialing Numbers (ADN), Last Numbers Dialed (LND), Location Information (LOCI), EMS

NIST - Summary

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 NIST guides are for the most part outdated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

Outline

Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective

6^{th} International Conference on E-Governance

Rizwan Ahmed and Rajiv V. Dharaskar

Outline

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 *[1][2]*

1. *(Aljazeera 2005) Phone Dealers in al-Hariri Probe*
   http://www.english.aljazeera.net/archive/2005/09/200841014558113928.html
2. *(ABC News 2011) Michael Jackson's Slurred Speech Heard in Court*
   http://abcnews.go.com/US/video/michael-jacksons-slurred-speech-heard-in-court-14617444

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

Outline

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

Outline

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

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! Therefore, 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

Differences - Tools and Toolkits

Problems

- Developed by third parties; not independently verified or tested; use both manufacturer and self-developed commands to gain access; support limited number of devices; direct access is not achievable

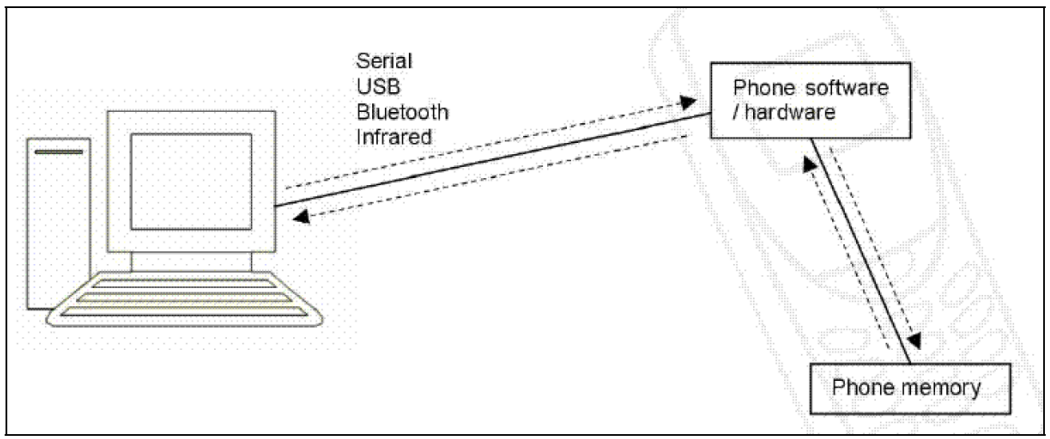


Figure 1: Indirect Access to Data in Mobile Phone Memory via Software and Hardware Commands and Methods (McCarthy, 2005).

1 *Graphic from Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective, Rizwan Ahmed and Rajiv V. Dharaskar*

Outline

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

Weaknesses - Procedure

UK Association of Chief Police Officers - Good Practice Guide for Computer based Electronic Evidence

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court
2. In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on a storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions
3. An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result
4. 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

Weaknesses - Procedure

International Organization on Computer Evidence (IOCE) - The Guidelines for Best Practice in the Forensic Examination of Digital Technology

1. The general rules of evidence should be applied to all digital evidence
2. Upon seizing digital evidence, actions taken should not change that evidence
3. When it is necessary for a person to access original digital evidence that person should be suitably trained for the purpose
4. All activity relation to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review
5. 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

Outline

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

Outline

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]*

1 *(Dharaskar 2011) http://www.dharaskar.com/*

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

1 *(Dharaskar 2011) http://www.dharaskar.com/*

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

1 *(Dharaskar 2011) http://www.dharaskar.com/*

Summary

1. Resolve conflicts and expand in digital evidence definitions
2. Create standardized digital evidence policy, guidelines, and methodologies
3. Require freer flow of information about OS, FS, and Forensic Tools

Outline

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

Outline

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

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

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

Overview - History

Year	Name	Description
2003	Willassen	Proposed extraction by desoldering memory chip and reading from programmer
2006	Casadei	SIM-brush tool (Linux and Windows)
2007	Kim	Tool to acquire data from Korean CDMA flash memory
2007	Al-Zarouni	Study of mobile phone flasher devices
2007	Oliver	Tool to acquire active files from Symbian OSv7
2008	Jansen	Baseline tool to populate SIM with test data
2009	Gaffaney	Evaluate iOS tools
2010	Husain	Analysis of iOS IM clients

Outline

Model

System Model

- Message Script Generator (MSG)
- UI/Application Exerciser Monkey
- Chat Bot
- Memory Acquisition Tool (memgrab)
- Memory Dump Analyser (MDA)

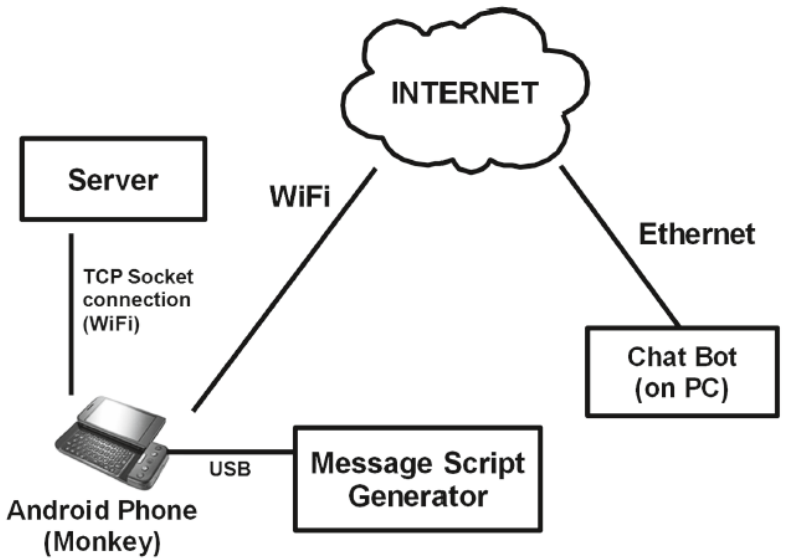


Fig. 1 – System overview.

1 *Graphic from Live memory forensics of mobile phones, Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Change*

Model - MSG and Monkey

MSG and Monkey

1. Message Script Generator (MSG)
   - Randomly generates test message and monkey script
2. UI Application Exerciser Monkey
   - Part of Android software stack
   - Use to perform pseudo-random actions on phone
   - Can perform deterministic actions through Android Debug Bridge (ADB)

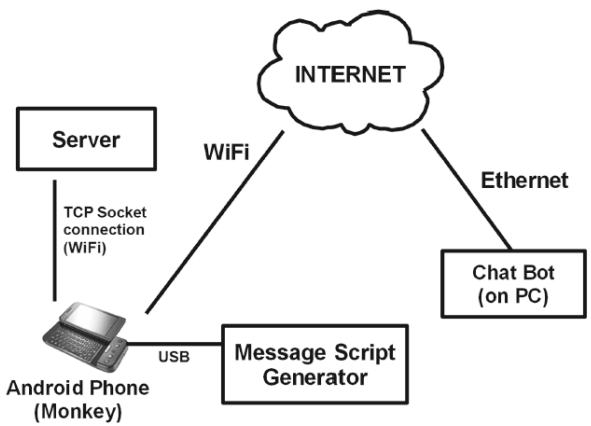


Fig. 1 – System overview.

1. *Graphic from Live memory forensics of mobile phones, Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Change*

Model - Chat Bot

Chat Bot

- Java console-based app that uses the Smack API
- Smack API is a Java library for IM clients using Extensible Messaging and Presence Protocol (XMPP)
- Configurable message length, character set, and interval between messages

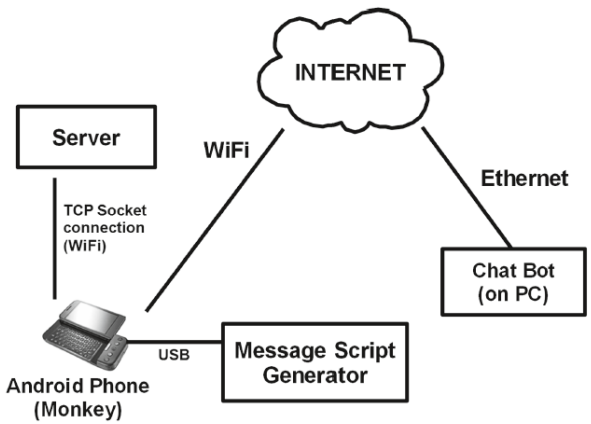


Fig. 1 – System overview.

1 *Graphic from Live memory forensics of mobile phones, Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Change*

Model - Memory Acquisition Tool (memgrab)

Memory Acquisition Tool (memgrab)

- Process memory management is handled by the Linux 2.6 kernel
- Anonymous shared memory is handled by ashmem driver instead of the Linux kernel IPC module
- Low Memory Killer driver replaces the standard Out-of-Memory Killer module
- Relies on /proc/pid/maps (addresses) and /proc/pid/mem (memory)
- Performs Process Trace (ptrace) system call (traces by controlling exec)

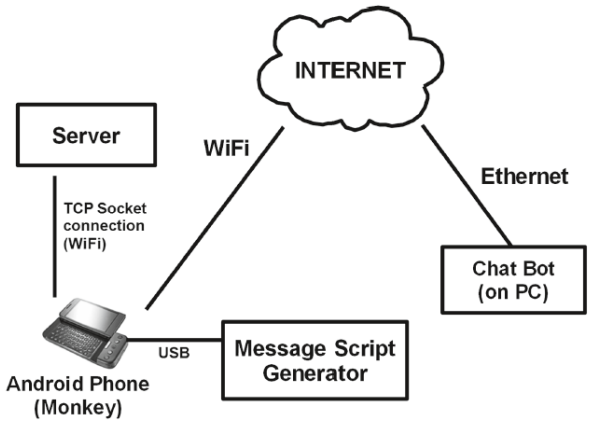


Fig. 1 – System overview.

1 *Graphic from Live memory forensics of mobile phones, Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Change*

Model - Memory Dump Analyser (MDA)

Memory Dump Analyser (MDA)

In the memory dump, the outgoing message appears in two forms (i.e. before and after processing to be sent as a network packet to the chat server).

[“m”,“userone@gmail.com/Smack
-> F0FBEF9E”,“MESSAGE”,“MSG_ID”,“c”]]

and

[[1011,[“c”,[’4890438E28A0973D’,[“m”,“
-> userone@gmail.com/SmackF0FBEF9E”
->,“MESSAGE”,“”,“s”,[“MESSAGE”]

while the incoming message appears in one form:

[[1013,[“c”,[’4890438E28A0973D’,[“m”,“
-> usertwo@gmail.com/SmackEC940444”
->,“MESSAGE”,“”,“r”,[“MESSAGE”]

We identify the common structure in the messages as:

[“m”,“USER_ID@gmail.com/XMPP_RESOURCE”,
-> “MESSAGE”,“

and use the following regular expression to capture the message contents.

[“m”,“[.a-zA-Z\d]+@gmail.com
-> [/a-zA-Z0-9]*“,”(.*);

Based on a list of the generated messages, the MDA consists of Perl scripts to perform searches on each dump. The results of the findings of whole or partial messages are then compiled into a report.

1 *Graphic from Live memory forensics of mobile phones, Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Change*

Outline

Experiments - Process Memory Region Investigation

Process Memory Region Investigation

- 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

Experiments - Cached Data Examination

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

Experiments - Realistic Parameters (1 of 4)

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

Experiments - Realistic Parameters (2 of 4)

Character Set

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

Experiments - Realistic Parameters (3 of 4)

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

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.

Experiments - Realistic Parameters (4 of 4)

No-wait Scenario Interval

(key) x (length - 1)

Wait Scenario Interval

(2 x key) x (length - 1)

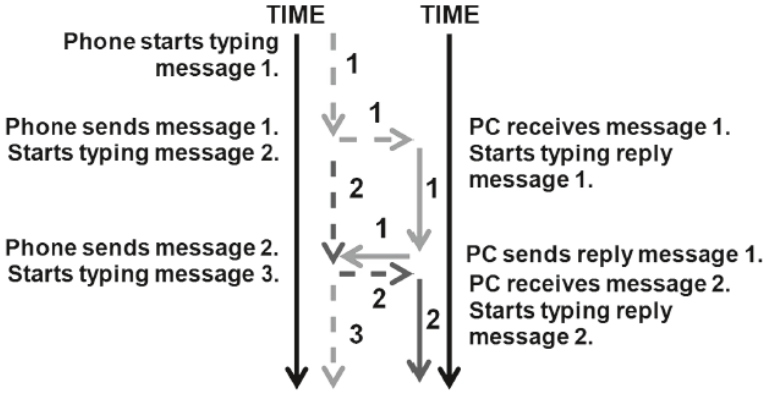


Fig. 2 – No-wait scenario.

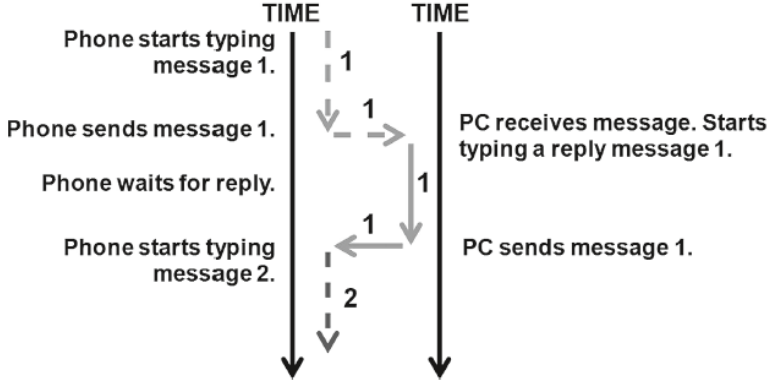


Fig. 3 – Waiting scenario.

1 *Graphic from Live memory forensics of mobile phones, Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Change*

Experiments - Evidence Persistency Examination

Evidence Persistency Examination (Outgoing)

Scenario: Wait, Length: 75, Key: 500 ms, Odd ID: Sent, Even ID: Received

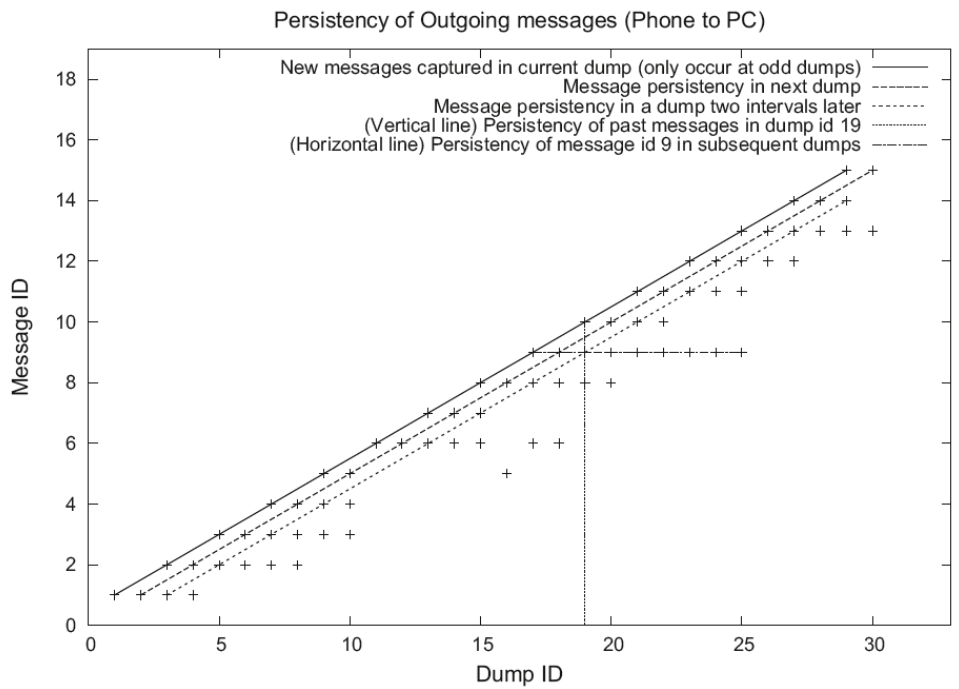


Fig. 4 – Persistency of outgoing messages.

1 *Graphic from Live memory forensics of mobile phones, Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Change*

Experiments - Evidence Persistency Examination

Evidence Persistency Examination (Incoming)

Scenario: Wait, Length: 75, Key: 500 ms, Odd ID: Sent, Even ID: Received

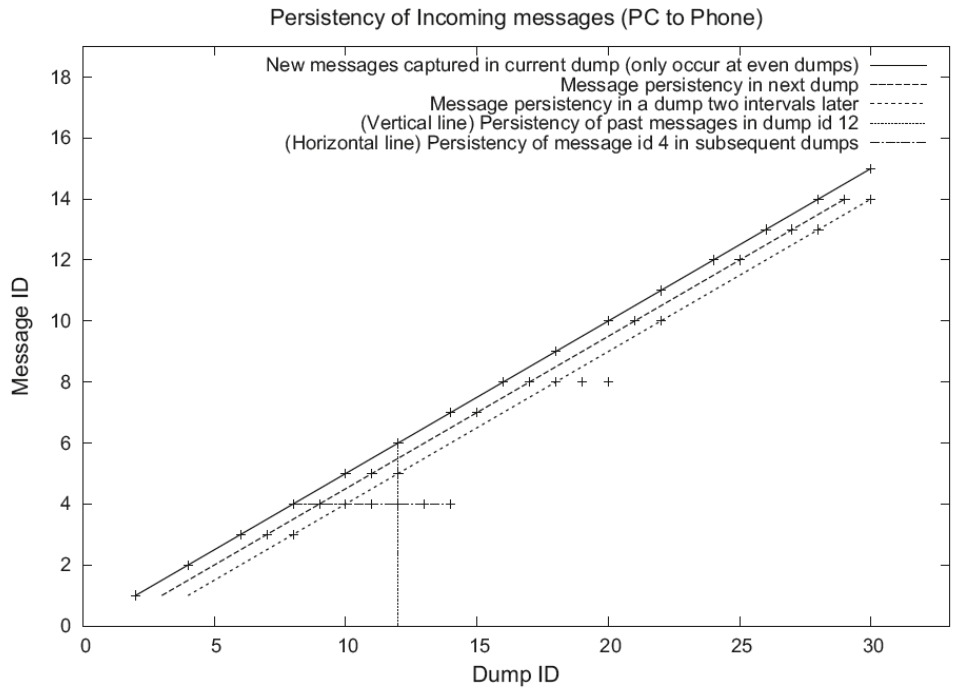


Fig. 5 – Persistency of incoming messages.

1 *Graphic from Live memory forensics of mobile phones, Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Change*

Experiments - Memory Dump Interval Investigation

Results

- 100% of outgoing messages can be acquired at ANY dump interval
- 100% of incoming messages can be acquired at 5s dump interval
- As the dump interval increases incoming messages are lost
  (10s - 87%, 20s - 76%, 30s - 85%)
- Outgoing messages have a higher persistency than incoming messages
- Outgoing messages can exist in multiple copies and formats
- Incoming messages can exist in at most two copies and one format

Table 1 – Captured (whole) messages in waiting scenario with dump intervals of 40 and 60 s.

Message length (Chars)	Dump interval			
	40 s		60 s	
	Outgoing Msgs	Incoming Msgs	Outgoing Msgs	Incoming Msgs
75	15/15	15/15	15/15	13/15
150	15/15	15/15	15/15	15/15
225	15/15	14/15	15/15	15/15

Table 2 – Captured (whole) messages in no-wait scenario with dump intervals of 5 and 10 s.

Message length (Chars)	Dump interval			
	5 s		10 s	
	Outgoing Msgs	Incoming Msgs	Outgoing Msgs	Incoming Msgs
75	15/15	15/15	15/15	13/15
150	15/15	15/15	15/15	13/15
225	15/15	15/15	15/15	13/15

Table 3 – Captured (whole) messages in no-wait scenario with dump intervals of 20 and 30 s.

Message length (Chars)	Dump interval			
	20 s		30 s	
	Outgoing Msgs	Incoming Msgs	Outgoing Msgs	Incoming Msgs
75	15/15	11/15	15/15	12/15
150	15/15	13/15	15/15	13/15
225	15/15	10/15	15/15	13/15

1 *Graphic from Live memory forensics of mobile phones, Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Change*

Outline

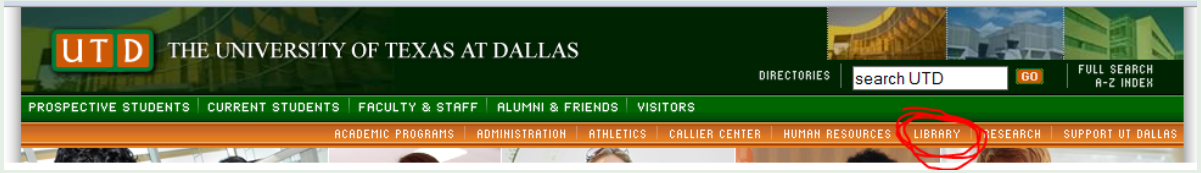
Conclusions

1. Live memory forensic analysis on mobile devices allows for the recovery of evidence that resides in volatile memory (in this case communication based messages)
2. This technique avoids loss of important evidence, optimizes processing time, and circumvents encryption and obfuscation techniques
3. 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

Outline

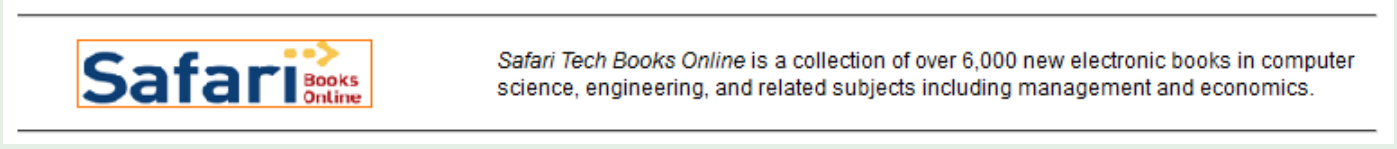
Extras - Safari

UTD - http://www.utdallas.edu

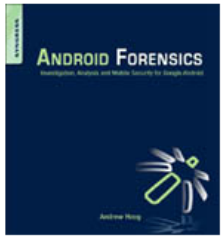


Library

Safari



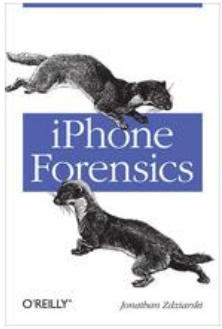
Extras - Books



< Return to Search Results

Android Forensics: Investigation, Analysis, and Mobile Security for Google Android

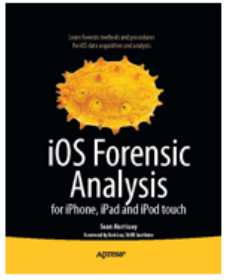
By: Andrew Hoog
Publisher: Syngress
Pub. Date: June 15, 2011
Print ISBN-13: 978-1-59749-651-3
E-Book ISBN-13: 978-1-59749-652-0
Pages in Print Edition: 393
Amazon.com® Reviews
Subscriber Rating: ☆☆☆☆☆ **[1 Rating]** Subscriber Reviews



< Return to Search Results

iPhone Forensics

By: Jonathan Zdziarski
Publisher: O'Reilly Media, Inc.
Pub. Date: September 12, 2008
Print ISBN-13: 978-0-596-15358-8
Pages in Print Edition: 144
Amazon.com® Reviews
Subscriber Rating: ☆☆☆☆☆ **[2 Ratings]**



< Return to Search Results

iOS Forensic Analysis for iPhone, iPad, and iPod touch

By: Sean Morrissey
Publisher: Apress
Pub. Date: December 27, 2010
Print ISBN: 978-1-4302-3342-8
Web ISBN: 1-4302-3342-7
Pages in Print Edition: 370
Amazon.com® Reviews
Subscriber Rating: ☆☆☆☆☆ **[0 Ratings]**