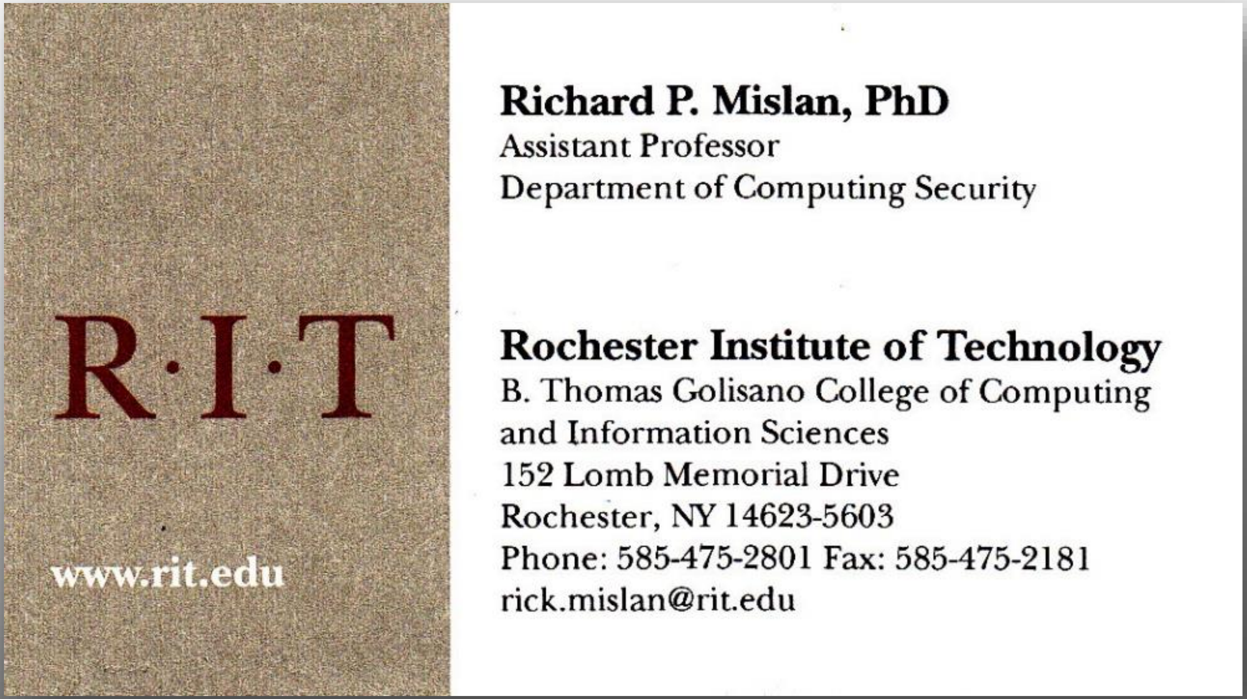
Mobile Device Forensics in Academia

How we find out what we need to find out.

National Institute of Standards and Technology
U.S. Department of Commerce

Mobile Device Forensics in Academia



R·I·T

www.rit.edu

Richard P. Mislan, PhD
Assistant Professor
Department of Computing Security

Rochester Institute of Technology
B. Thomas Golisano College of Computing
and Information Sciences
152 Lomb Memorial Drive
Rochester, NY 14623-5603
Phone: 585-475-2801 Fax: 585-475-2181
rick.mislan@rit.edu

Academia

ac·a·de·mi·a /ˌakəˈdēmēə/

Noun. Origin 1945–50; Neo-Latin

the environment concerned with the pursuit of Research, Education, and Scholarship.

"Study the past if you would define the future...."

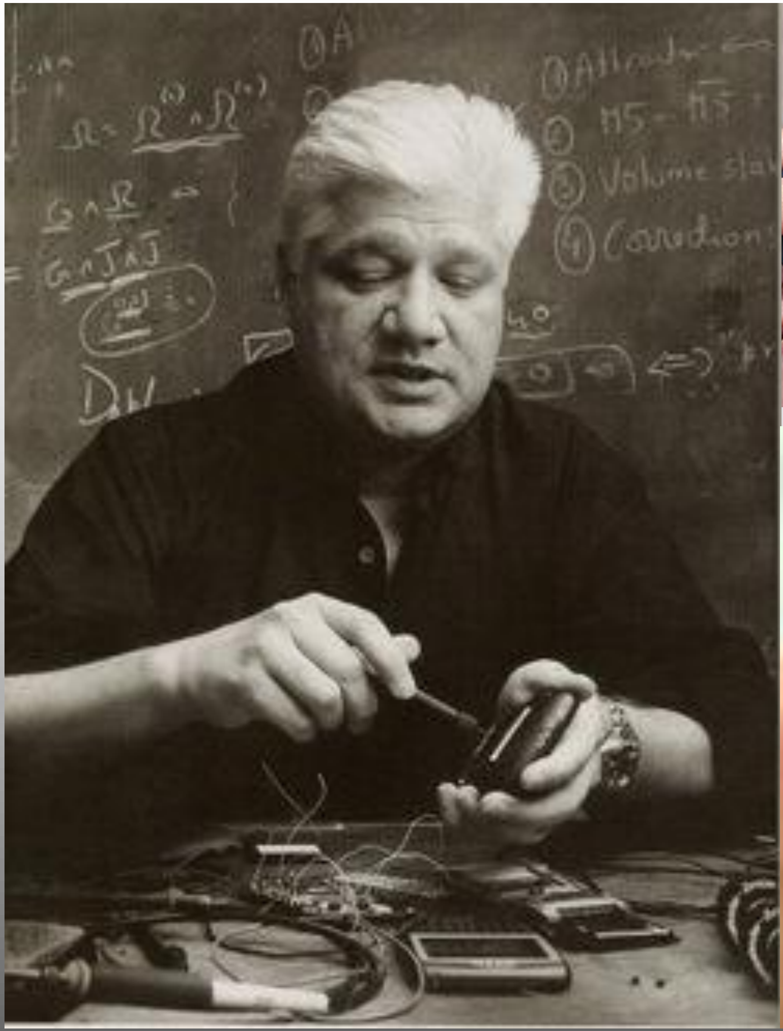
- Confucius

BACK TO THE FUTURE

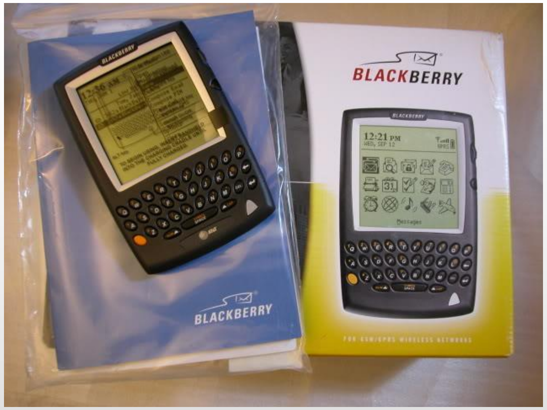
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

2000

In 2002…


Volume
Condition

RIM
10:04 AM
BLACKBERRY

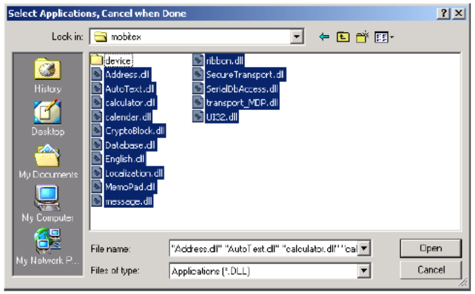

BLACKBERRY
BLACKBERRY
12:21 PM
BLACKBERRY

RIM
12:27 AM

Michael Burnette

Forensic Examination of a RIM (BlackBerry) Wireless Device
June, 2002

Michael W. Burnette
Director of Information Technology
Rogers & Hardin LLP
mwb@rh-law.com



Select Applications, Cancel when Done

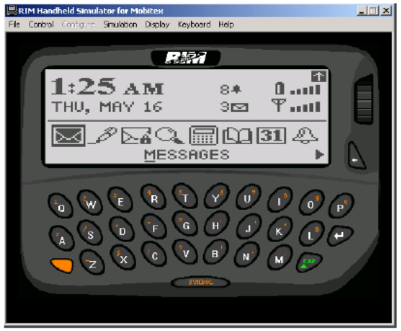
Look in: mobitex

device
Address.dll
AutoText.dll
calculator.dll
calendar.dll
CryptoBlock.dll
Database.dll
English.dll
Localization.dll
MemoPad.dll
message.dll
ribbon.dll
SecureTransport.dll
SerialDbAccess.dll
transport_MDP.dll
UI32.dll

File name: "Address.dll" "AutoText.dll" "calculator.dll" "cal

Files of type: Applications (*.DLL)

Run the simulator by choosing "control," "start simulation." If any prompt settings are checked on the control file menu, the system asks for the options above to be set one more time. The Simulator operates in exactly the same manner as a handheld BlackBerry with the additional convenience of PC keyboard manipulation.

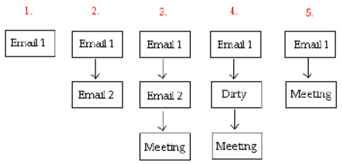


RIM Handheld Simulator for Mobitex

Erase: Condition, Rewrite to 1's only in 65K blocks.

Rewrite: Save 64K block to SRAM, erase 64K block of
write back to erased Flash block. This takes approximate

It goes without saying that the hardware is optimized for
best use of the hardware available by implementing a log
written in a linked list one at a time, each being appended to the last or the "end of the log". Each file or record has its own unique identifier, a number between 0 and 65536. When a change is necessary to an existing record, the original record is marked as dirty (bit twiddling most likely)[4] and the new version is written to the end of the file system with a new unique identifier. This process eliminates the need for on-the-fly erasures which cost a great deal of time. Periodically, the OS will clean old records marked as dirty, and defragment the file system, if necessary, to allow for more room for the file system to grow (expand the log). Once the end of address space is reached, the log wraps back around to the beginning of the address space. Unlike traditional file systems, fragmentation occurs in one direction only. Even if the first part of a file is near the end of address space and the next part wraps back around to the beginning, the virtual address space is the log, which is in one direction only.[11]



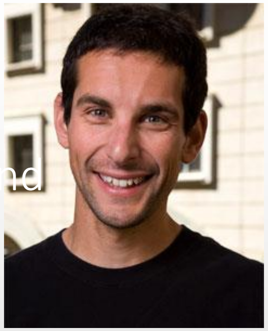
1. Email 1 is received and written to the file system
2. Email 2 is received and appended to the file system
3. Item is added to the calendar and is appended to the file system
4. Email 2 is deleted
5. File system cleanup occurs at next reset or when out of space

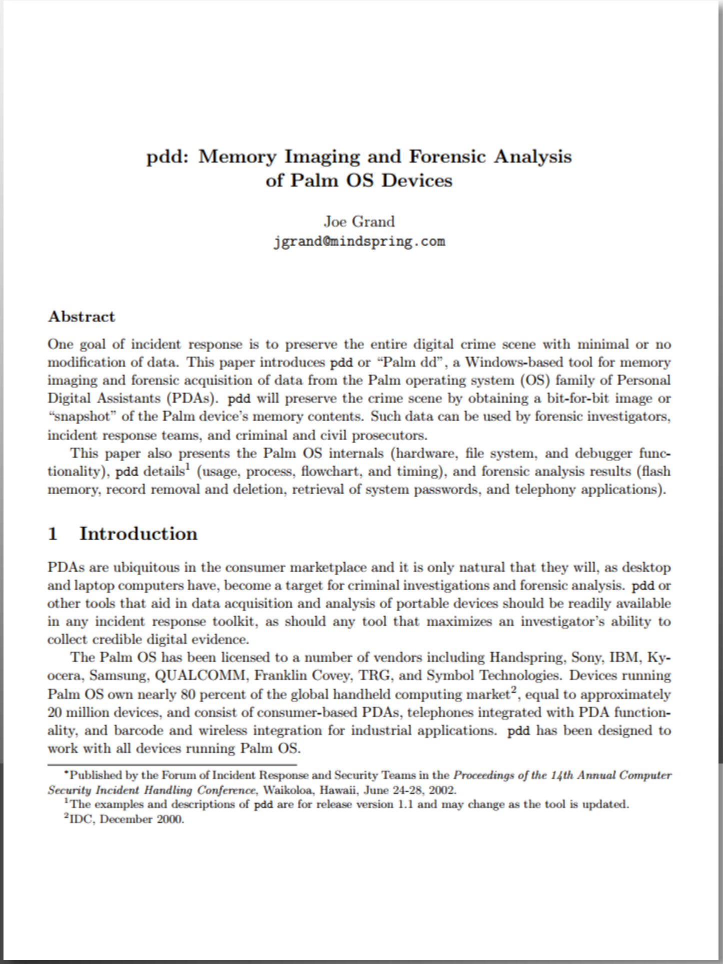
The log based file system and its interaction with the standard applications has notable ramifications when it comes to recovering whole files that either cross 64K sector boundaries or for which storage has been written several times. Take for instance the case of receiving a large email:

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

National Institute of Standards and Technology
U.S. Department of Commerce

Palm DD (PDD) – Joe Grand





pdd: Memory Imaging and Forensic Analysis of Palm OS Devices

Joe Grand
jgrand@mindspring.com

Abstract

One goal of incident response is to preserve the entire digital crime scene with minimal or no modification of data. This paper introduces pdd or "Palm dd", a Windows-based tool for memory imaging and forensic acquisition of data from the Palm operating system (OS) family of Personal Digital Assistants (PDAs). pdd will preserve the crime scene by obtaining a bit-for-bit image or "snapshot" of the Palm device's memory contents. Such data can be used by forensic investigators, incident response teams, and criminal and civil prosecutors.

This paper also presents the Palm OS internals (hardware, file system, and debugger functionality), pdd details[1] (usage, process, flowchart, and timing), and forensic analysis results (flash memory, record removal and deletion, retrieval of system passwords, and telephony applications).

1 Introduction

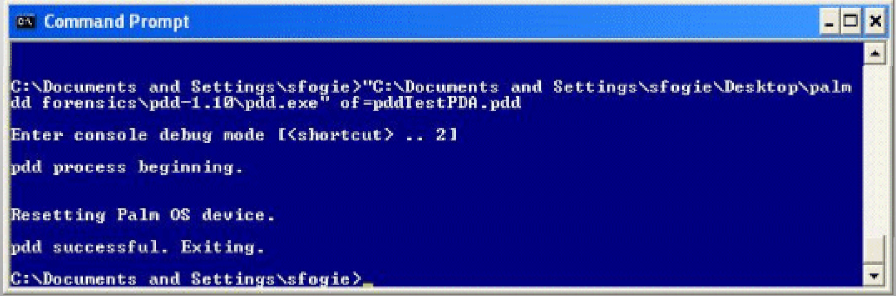
PDAs are ubiquitous in the consumer marketplace and it is only natural that they will, as desktop and laptop computers have, become a target for criminal investigations and forensic analysis. pdd or other tools that aid in data acquisition and analysis of portable devices should be readily available in any incident response toolkit, as should any tool that maximizes an investigator's ability to collect credible digital evidence.

The Palm OS has been licensed to a number of vendors including Handspring, Sony, IBM, Kyocera, Samsung, QUALCOMM, Franklin Covey, TRG, and Symbol Technologies. Devices running Palm OS own nearly 80 percent of the global handheld computing market[2], equal to approximately 20 million devices, and consist of consumer-based PDAs, telephones integrated with PDA functionality, and barcode and wireless integration for industrial applications. pdd has been designed to work with all devices running Palm OS.

[*] Published by the Forum of Incident Response and Security Teams in the *Proceedings of the 14th Annual Computer Security Incident Handling Conference*, Waikoloa, Hawaii, June 24-28, 2002.

[1] The examples and descriptions of pdd are for release version 1.1 and may change as the tool is updated.

[2] IDC, December 2000.

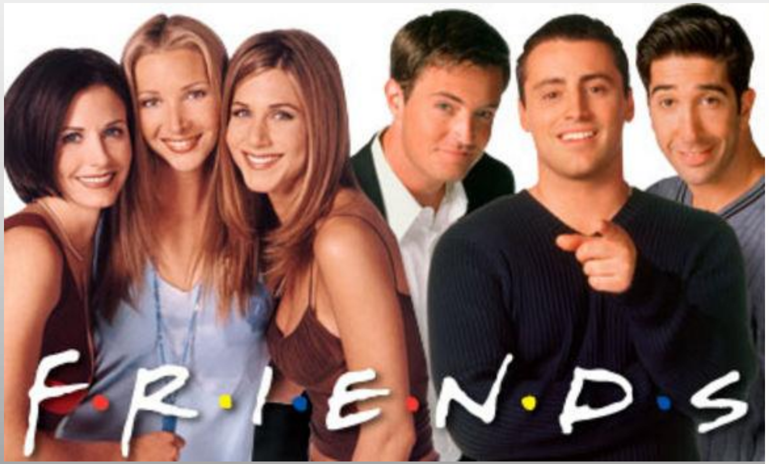


```
C:\Documents and Settings\sfogie>"C:\Documents and Settings\sfogie\Desktop\palm
dd forensics\pdd-1.10\pdd.exe" of=pddTestPDA.pdd

Enter console debug mode [<shortcut> .. 2]

pdd process beginning.

Resetting Palm OS device.

pdd successful. Exiting.

C:\Documents and Settings\sfogie>_
```

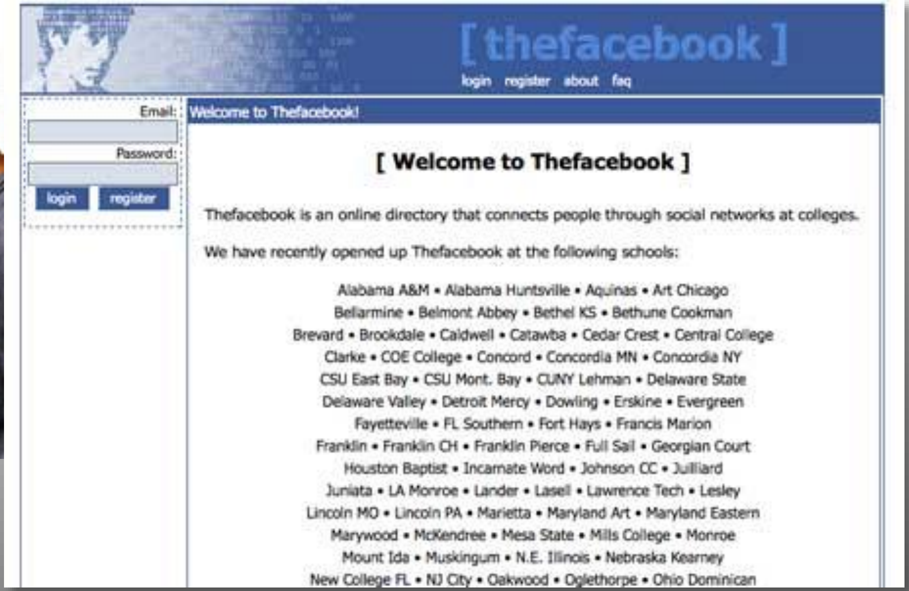
ROM.txt RAM.txt

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

2 years later…



2004



Welcome to Thefacebook!

[Welcome to Thefacebook]

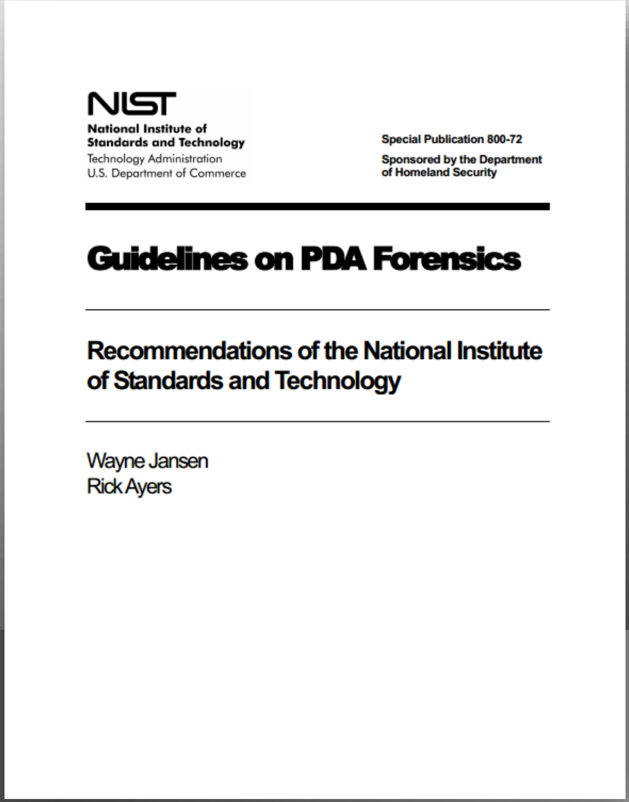
Thefacebook is an online directory that connects people through social networks at colleges.

We have recently opened up Thefacebook at the following schools:

Alabama A&M • Alabama Huntsville • Aquinas • Art Chicago
Bellarmine • Belmont Abbey • Bethel KS • Bethune Cookman
Brevard • Brookdale • Caldwell • Catawba • Cedar Crest • Central College
Clarke • COE College • Concord • Concordia MN • Concordia NY
CSU East Bay • CSU Mont. Bay • CUNY Lehman • Delaware State
Delaware Valley • Detroit Mercy • Dowling • Erskine • Evergreen
Fayetteville • FL Southern • Fort Hays • Francis Marion
Franklin • Franklin CH • Franklin Pierce • Full Sail • Georgian Court
Houston Baptist • Incarnate Word • Johnson CC • Julliard
Juniata • LA Monroe • Lander • Lasell • Lawrence Tech • Lesley
Lincoln MO • Lincoln PA • Marietta • Maryland Art • Maryland Eastern
Marywood • McKendree • Mesa State • Mills College • Monroe
Mount Ida • Muskingum • N.E. Illinois • Nebraska Kearney
New College FL • NJ City • Oakwood • Oglethorpe • Ohio Dominican

Rick Ayers & Wayne Jansen

August 2004



National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

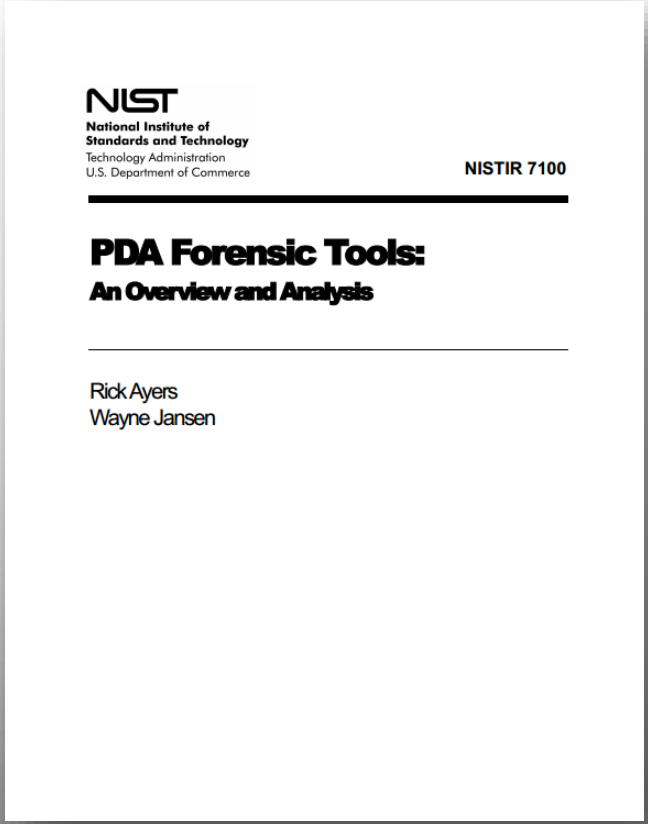
Special Publication 800-72

Sponsored by the Department of Homeland Security

Guidelines on PDA Forensics

Recommendations of the National Institute of Standards and Technology

Wayne Jansen
Rick Ayers



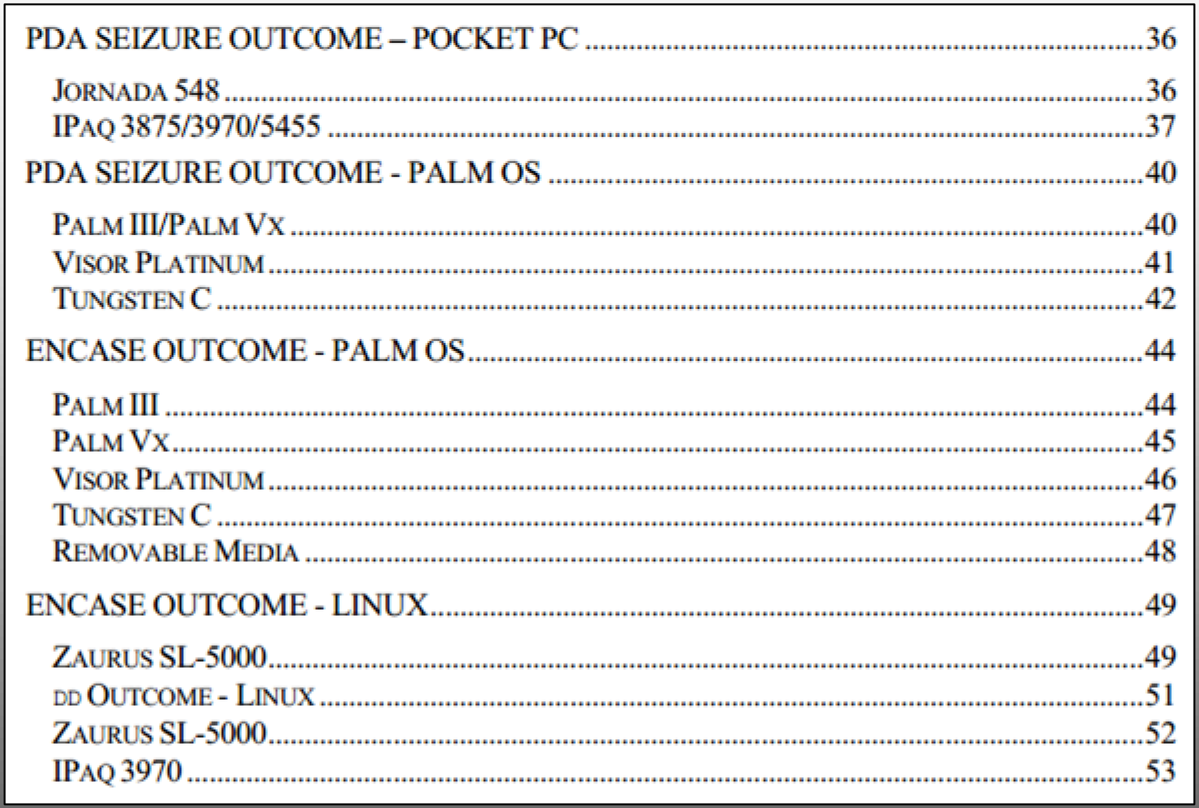
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

NISTIR 7100

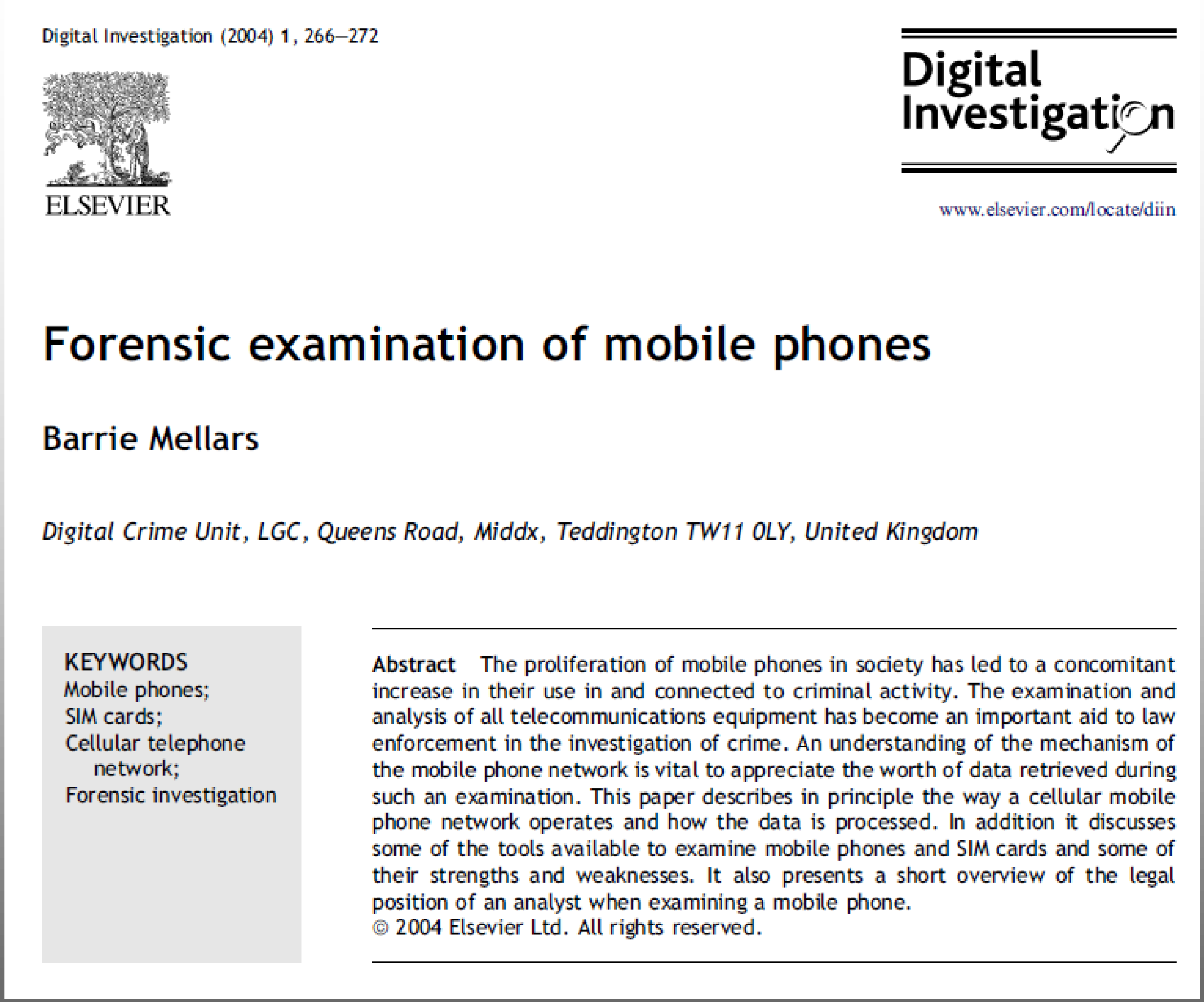
PDA Forensic Tools:
An Overview and Analysis

Rick Ayers
Wayne Jansen

Tools and Operating Systems – THEN…



NOKIA 5140
NOKIA 3610
1124



Digital Investigation (2004) 1, 266–272

ELSEVIER

Digital Investigation

www.elsevier.com/locate/diin

Forensic examination of mobile phones

Barrie Mellars

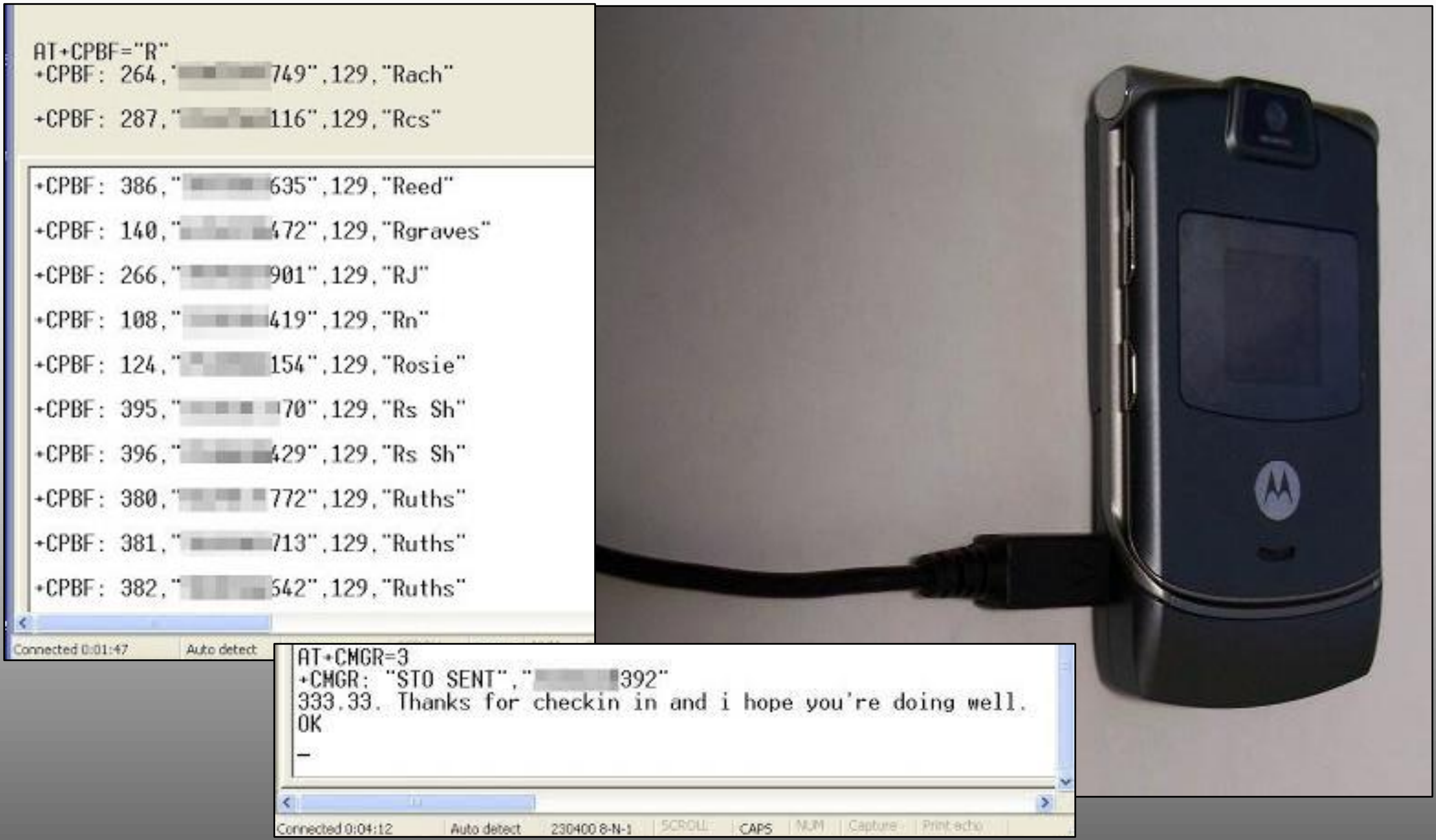
Digital Crime Unit, LGC, Queens Road, Middx, Teddington TW11 0LY, United Kingdom

KEYWORDS
Mobile phones;
SIM cards;
Cellular telephone network;
Forensic investigation

Abstract The proliferation of mobile phones in society has led to a concomitant increase in their use in and connected to criminal activity. The examination and analysis of all telecommunications equipment has become an important aid to law enforcement in the investigation of crime. An understanding of the mechanism of the mobile phone network is vital to appreciate the worth of data retrieved during such an examination. This paper describes in principle the way a cellular mobile phone network operates and how the data is processed. In addition it discusses some of the tools available to examine mobile phones and SIM cards and some of their strengths and weaknesses. It also presents a short overview of the legal position of an analyst when examining a mobile phone.

Barrie Mellars

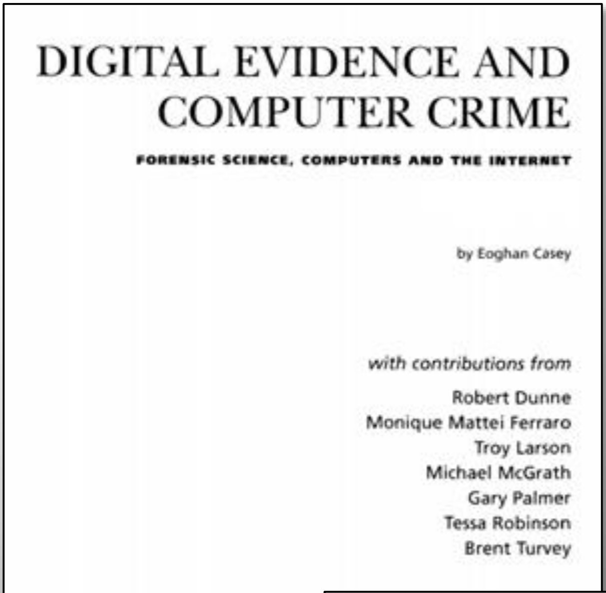
NIST
National Institute of Standards and Technology
U.S. Department of Commerce



```
AT+CPBF="R"
+CPBF: 264,"[redacted]749",129,"Rach"

+CPBF: 287,"[redacted]116",129,"Rcs"

+CPBF: 386,"[redacted]635",129,"Reed"

+CPBF: 140,"[redacted]472",129,"Rgraves"

+CPBF: 266,"[redacted]901",129,"RJ"

+CPBF: 108,"[redacted]419",129,"Rn"

+CPBF: 124,"[redacted]154",129,"Rosie"

+CPBF: 395,"[redacted]70",129,"Rs Sh"

+CPBF: 396,"[redacted]429",129,"Rs Sh"

+CPBF: 380,"[redacted]772",129,"Ruths"

+CPBF: 381,"[redacted]713",129,"Ruths"

+CPBF: 382,"[redacted]542",129,"Ruths"
```

```
AT+CMGR=3
+CMGR: "STO SENT","[redacted]392"
333.33. Thanks for checkin in and i hope you're doing well.
OK
_
```

AT Commands



DIGITAL EVIDENCE AND COMPUTER CRIME

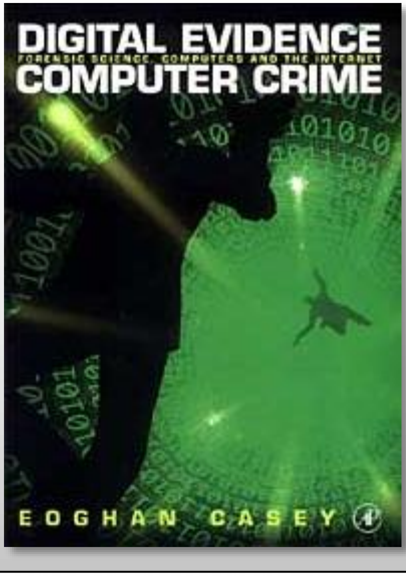
FORENSIC SCIENCE, COMPUTERS AND THE INTERNET

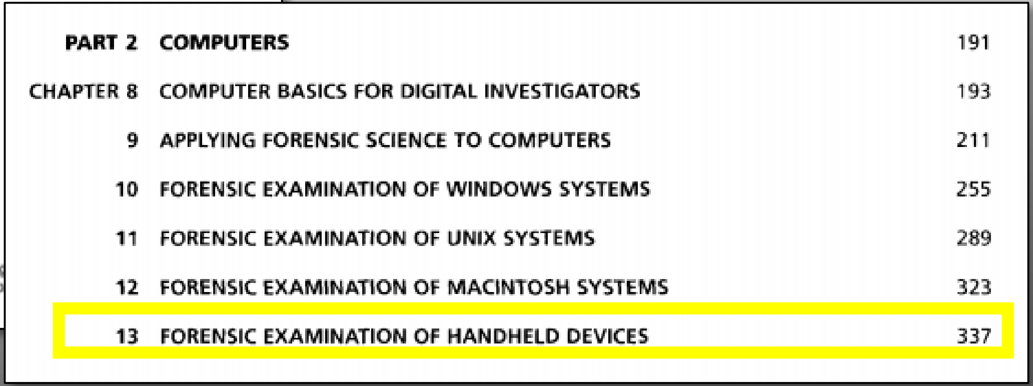
by Eoghan Casey

with contributions from

Robert Dunne
Monique Mattei Ferraro
Troy Larson
Michael McGrath
Gary Palmer
Tessa Robinson
Brent Turvey

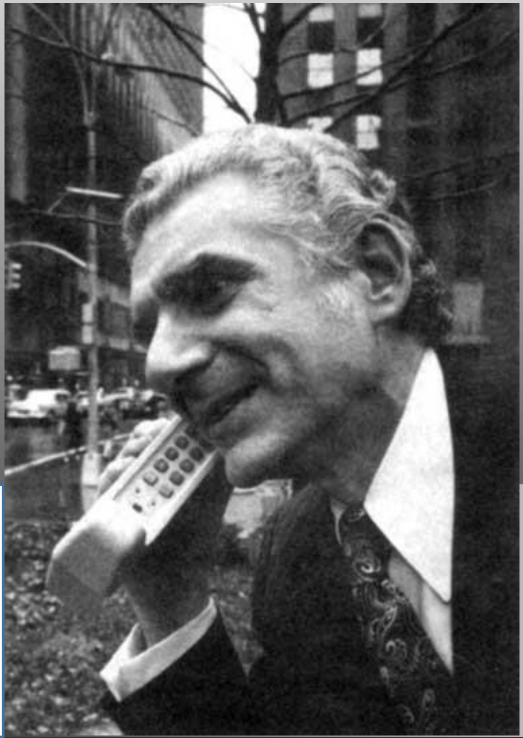
Amsterdam • Boston • Heidelberg
Paris • San Diego • San Francisco





Eoghan Casey

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

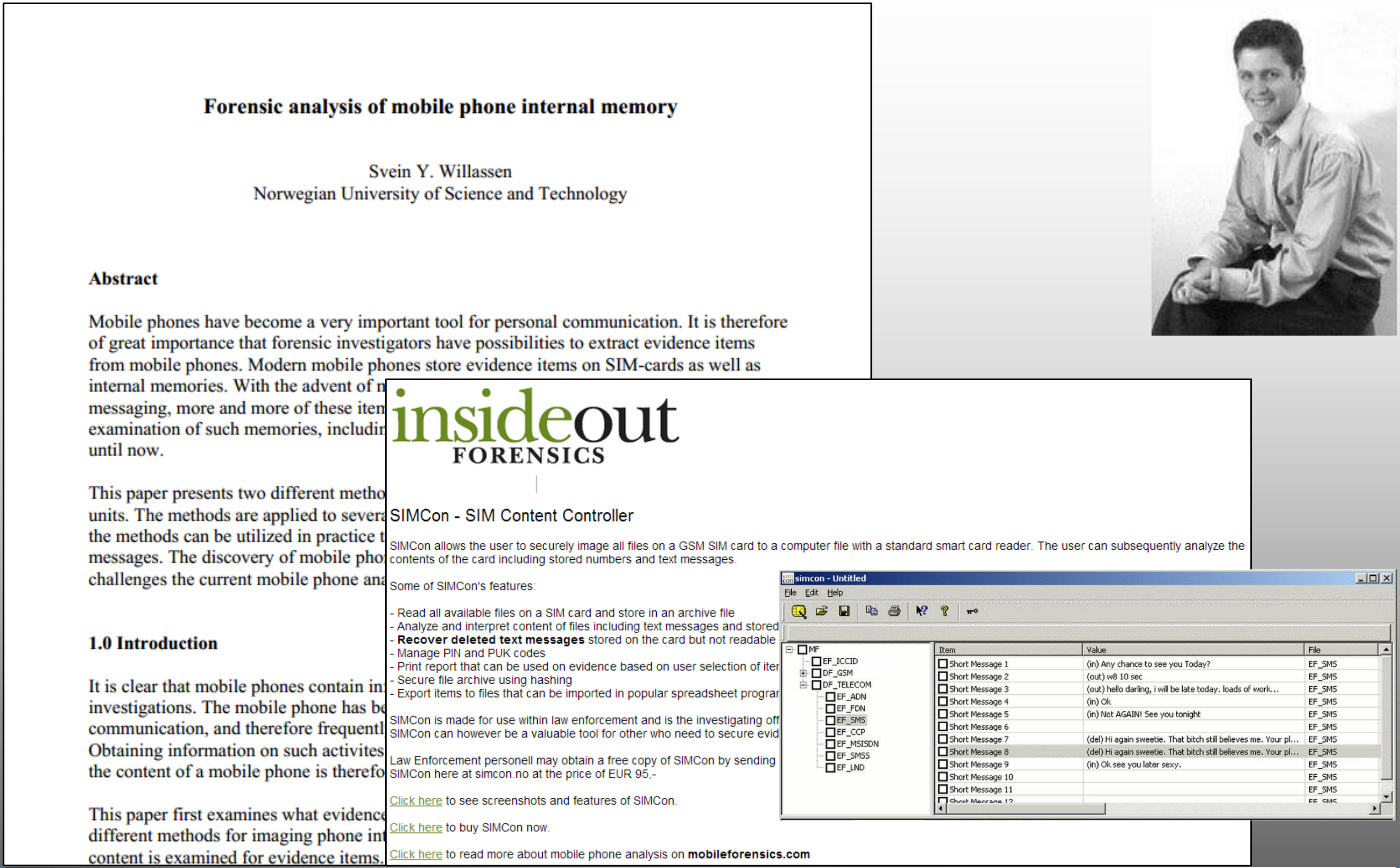


NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Mobile Forensics in Academia

- SIMs
- Shielding
- SMS
- GPS
- Hashing
- Images/Videos
- Legal

- Operating Systems
  - Android
  - BlackBerry
  - iOS
  - Maemo
  - Symbian
  - WebOS
  - Windows
- Other…



Forensic analysis of mobile phone internal memory

Svein Y. Willassen
Norwegian University of Science and Technology

Abstract

Mobile phones have become a very important tool for personal communication. It is therefore of great importance that forensic investigators have possibilities to extract evidence items from mobile phones. Modern mobile phones store evidence items on SIM-cards as well as internal memories. With the advent of n
messaging, more and more of these item
examination of such memories, includir
until now.

This paper presents two different metho
units. The methods are applied to severa
the methods can be utilized in practice t
messages. The discovery of mobile pho
challenges the current mobile phone ana

1.0 Introduction

It is clear that mobile phones contain in
investigations. The mobile phone has be
communication, and therefore frequentl
Obtaining information on such activites
the content of a mobile phone is therefo

This paper first examines what evidence
different methods for imaging phone in
content is examined for evidence items.

insideout
FORENSICS

SIMCon - SIM Content Controller

SIMCon allows the user to securely image all files on a GSM SIM card to a computer file with a standard smart card reader. The user can subsequently analyze the contents of the card including stored numbers and text messages.

Some of SIMCon's features:

- Read all available files on a SIM card and store in an archive file
- Analyze and interpret content of files including text messages and stored
- **Recover deleted text messages** stored on the card but not readable
- Manage PIN and PUK codes
- Print report that can be used on evidence based on user selection of iter
- Secure file archive using hashing
- Export items to files that can be imported in popular spreadsheet prograr

SIMCon is made for use within law enforcement and is the investigating off
SIMCon can however be a valuable tool for other who need to secure evid

Law Enforcement personell may obtain a free copy of SIMCon by sending
SIMCon here at simcon.no at the price of EUR 95,-

Click here to see screenshots and features of SIMCon.

Click here to buy SIMCon now.

Click here to read more about mobile phone analysis on **mobileforensics.com**

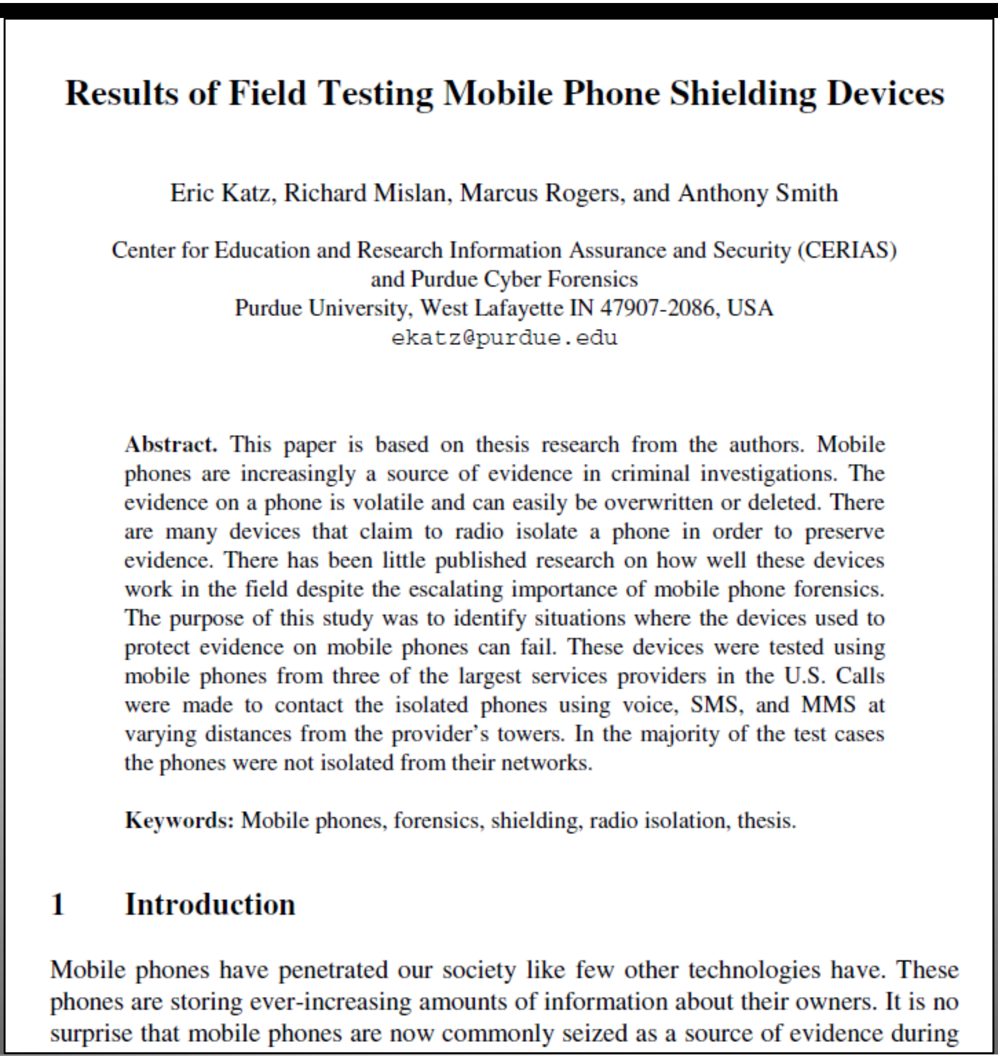
simcon - Untitled

Item	Value	File
□ Short Message 1	(in) Any chance to see you Today?	EF_SMS
□ Short Message 2	(out) w8 10 sec	EF_SMS
□ Short Message 3	(out) hello darling, i will be late today. loads of work...	EF_SMS
□ Short Message 4	(in) Ok	EF_SMS
□ Short Message 5	(in) Not AGAIN! See you tonight	EF_SMS
□ Short Message 6		EF_SMS
□ Short Message 7	(del) Hi again sweetie. That bitch still believes me. Your pl...	EF_SMS
□ Short Message 8	(del) Hi again sweetie. That bitch still believes me. Your pl...	EF_SMS
□ Short Message 9	(in) Ok see you later sexy.	EF_SMS
□ Short Message 10		EF_SMS
□ Short Message 11		EF_SMS
□ Short Message 12		EF_SMS

SIM

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Shielding



Results of Field Testing Mobile Phone Shielding Devices

Eric Katz, Richard Mislan, Marcus Rogers, and Anthony Smith

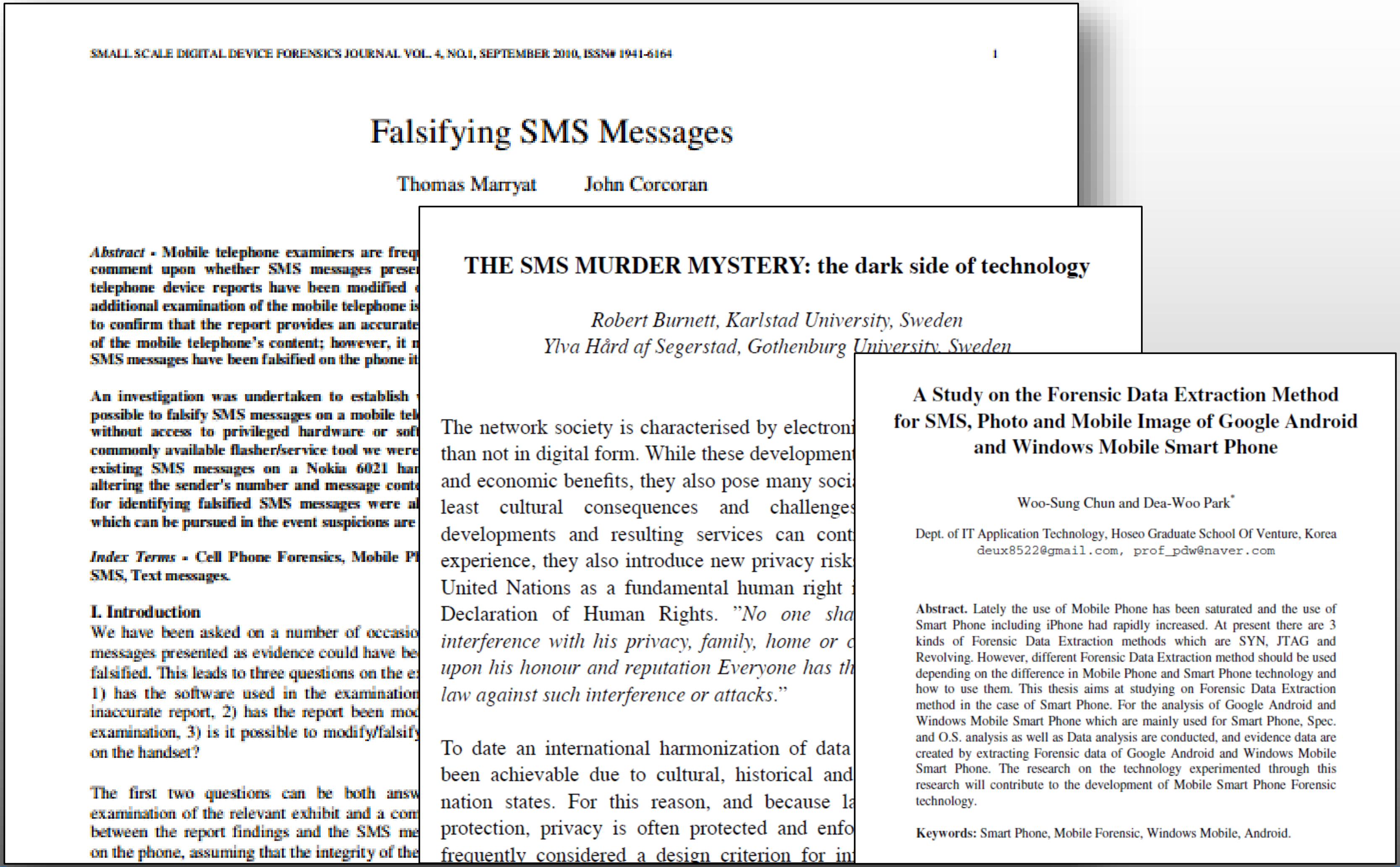
Center for Education and Research Information Assurance and Security (CERIAS)
and Purdue Cyber Forensics
Purdue University, West Lafayette IN 47907-2086, USA
ekatz@purdue.edu

Abstract. This paper is based on thesis research from the authors. Mobile phones are increasingly a source of evidence in criminal investigations. The evidence on a phone is volatile and can easily be overwritten or deleted. There are many devices that claim to radio isolate a phone in order to preserve evidence. There has been little published research on how well these devices work in the field despite the escalating importance of mobile phone forensics. The purpose of this study was to identify situations where the devices used to protect evidence on mobile phones can fail. These devices were tested using mobile phones from three of the largest services providers in the U.S. Calls were made to contact the isolated phones using voice, SMS, and MMS at varying distances from the provider's towers. In the majority of the test cases the phones were not isolated from their networks.

Keywords: Mobile phones, forensics, shielding, radio isolation, thesis.

1 Introduction

Mobile phones have penetrated our society like few other technologies have. These phones are storing ever-increasing amounts of information about their owners. It is no surprise that mobile phones are now commonly seized as a source of evidence during



SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL VOL. 4, NO.1, SEPTEMBER 2010, ISSN# 1941-6164 1

Falsifying SMS Messages

Thomas Marryat John Corcoran

Abstract - Mobile telephone examiners are freq
comment upon whether SMS messages prese
telephone device reports have been modified
additional examination of the mobile telephone is
to confirm that the report provides an accurate
of the mobile telephone's content; however, it n
SMS messages have been falsified on the phone it

An investigation was undertaken to establish
possible to falsify SMS messages on a mobile tel
without access to privileged hardware or soft
commonly available flasher/service tool we were
existing SMS messages on a Nokia 6021 han
altering the sender's number and message conte
for identifying falsified SMS messages were al
which can be pursued in the event suspicions are

Index Terms - Cell Phone Forensics, Mobile Ph
SMS, Text messages.

I. Introduction
We have been asked on a number of occasio
messages presented as evidence could have be
falsified. This leads to three questions on the e
1) has the software used in the examination
inaccurate report, 2) has the report been mod
examination, 3) is it possible to modify/falsify
on the handset?

The first two questions can be both answ
examination of the relevant exhibit and a com
between the report findings and the SMS me
on the phone, assuming that the integrity of the

THE SMS MURDER MYSTERY: the dark side of technology

Robert Burnett, Karlstad University, Sweden
Ylva Hård af Segerstad, Gothenburg University, Sweden

The network society is characterised by electroni
than not in digital form. While these development
and economic benefits, they also pose many soci
least cultural consequences and challenges
developments and resulting services can cont
experience, they also introduce new privacy risk
United Nations as a fundamental human right i
Declaration of Human Rights. "*No one sha
interference with his privacy, family, home or c
upon his honour and reputation Everyone has th
law against such interference or attacks.*"

To date an international harmonization of data
been achievable due to cultural, historical and
nation states. For this reason, and because la
protection, privacy is often protected and enfo
frequently considered a design criterion for in

A Study on the Forensic Data Extraction Method for SMS, Photo and Mobile Image of Google Android and Windows Mobile Smart Phone

Woo-Sung Chun and Dea-Woo Park*

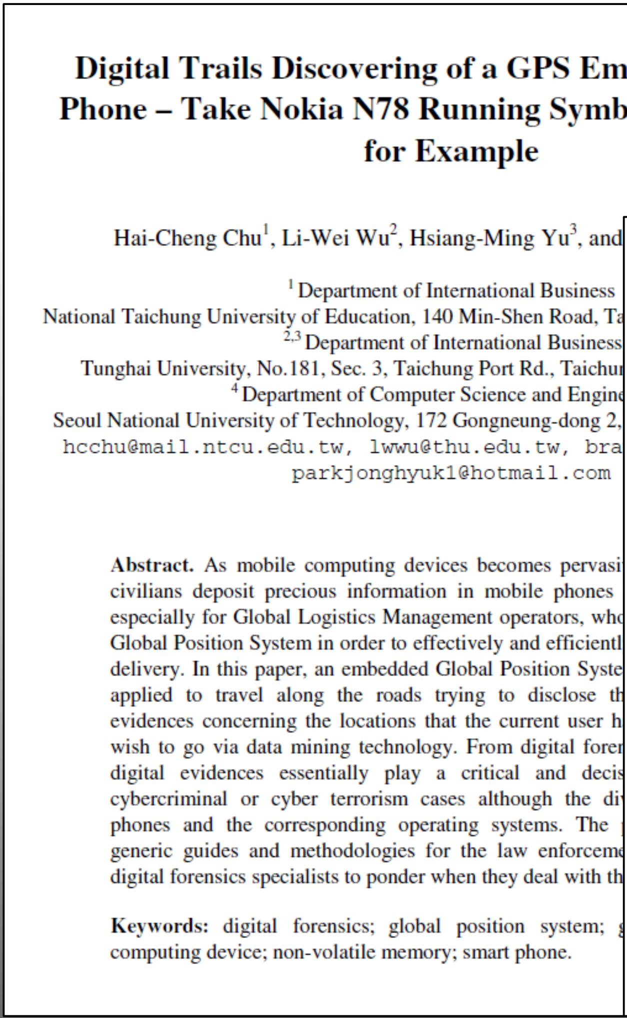
Dept. of IT Application Technology, Hoseo Graduate School Of Venture, Korea
deux8522@gmail.com, prof_pdw@naver.com

Abstract. Lately the use of Mobile Phone has been saturated and the use of Smart Phone including iPhone had rapidly increased. At present there are 3 kinds of Forensic Data Extraction methods which are SYN, JTAG and Revolving. However, different Forensic Data Extraction method should be used depending on the difference in Mobile Phone and Smart Phone technology and how to use them. This thesis aims at studying on Forensic Data Extraction method in the case of Smart Phone. For the analysis of Google Android and Windows Mobile Smart Phone which are mainly used for Smart Phone, Spec. and O.S. analysis as well as Data analysis are conducted, and evidence data are created by extracting Forensic data of Google Android and Windows Mobile Smart Phone. The research on the technology experimented through this research will contribute to the development of Mobile Smart Phone Forensic technology.

Keywords: Smart Phone, Mobile Forensic, Windows Mobile, Android.

SMS

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

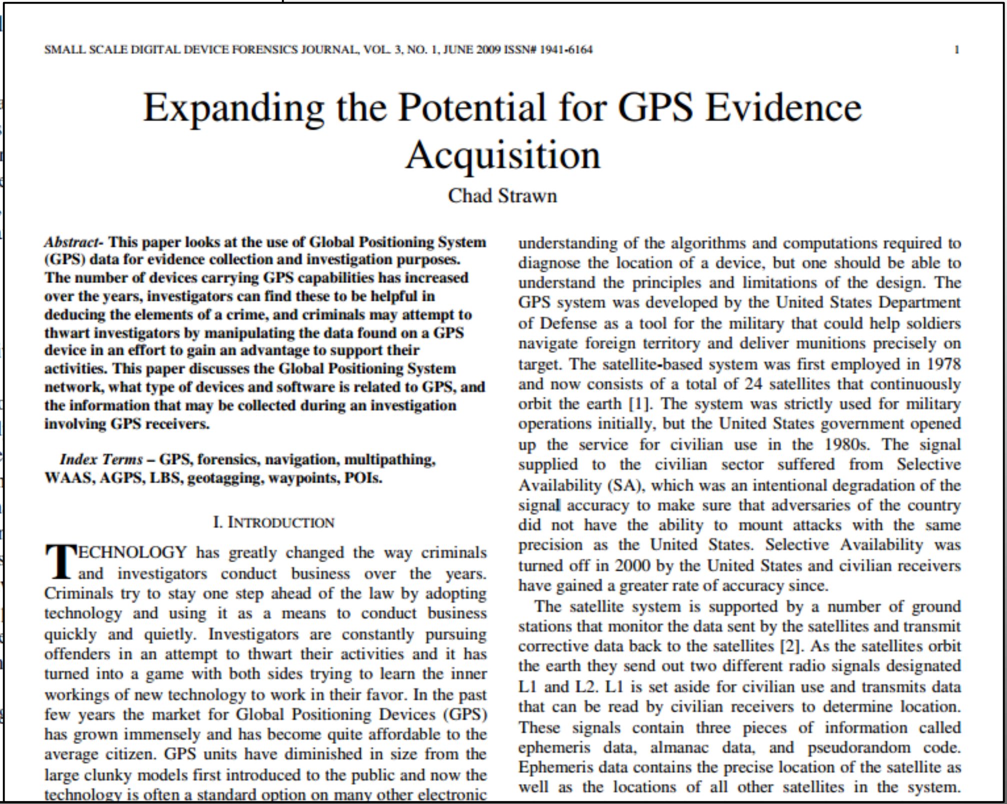

Digital Trails Discovering of a GPS Embedded Smart Phone – Take Nokia N78 Running Symbian S60 Ver 3.2 for Example

Hai-Cheng Chu[1], Li-Wei Wu[2], Hsiang-Ming Yu[3], and

[1] Department of International Business
National Taichung University of Education, 140 Min-Shen Road, Ta
[2,3] Department of International Business
Tunghai University, No.181, Sec. 3, Taichung Port Rd., Taichu
[4] Department of Computer Science and Engin
Seoul National University of Technology, 172 Gongneung-dong 2,
hcchu@mail.ntcu.edu.tw, lwwu@thu.edu.tw, bra
parkjonghyuk1@hotmail.com

Abstract. As mobile computing devices becomes pervasi
civilians deposit precious information in mobile phones
especially for Global Logistics Management operators, wh
Global Position System in order to effectively and efficient
delivery. In this paper, an embedded Global Position Syste
applied to travel along the roads trying to disclose th
evidences concerning the locations that the current user h
wish to go via data mining technology. From digital fore
digital evidences essentially play a critical and decis
cybercriminal or cyber terrorism cases although the di
phones and the corresponding operating systems. The
generic guides and methodologies for the law enforceme
digital forensics specialists to ponder when they deal with th

Keywords: digital forensics; global position system;
computing device; non-volatile memory; smart phone.


SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 3, NO. 1, JUNE 2009 ISSN# 1941-6164 1

Expanding the Potential for GPS Evidence Acquisition

Chad Strawn

Abstract- **This paper looks at the use of Global Positioning System (GPS) data for evidence collection and investigation purposes. The number of devices carrying GPS capabilities has increased over the years, investigators can find these to be helpful in deducing the elements of a crime, and criminals may attempt to thwart investigators by manipulating the data found on a GPS device in an effort to gain an advantage to support their activities. This paper discusses the Global Positioning System network, what type of devices and software is related to GPS, and the information that may be collected during an investigation involving GPS receivers.**

Index Terms **– GPS, forensics, navigation, multipathing, WAAS, AGPS, LBS, geotagging, waypoints, POIs.**

I. Introduction

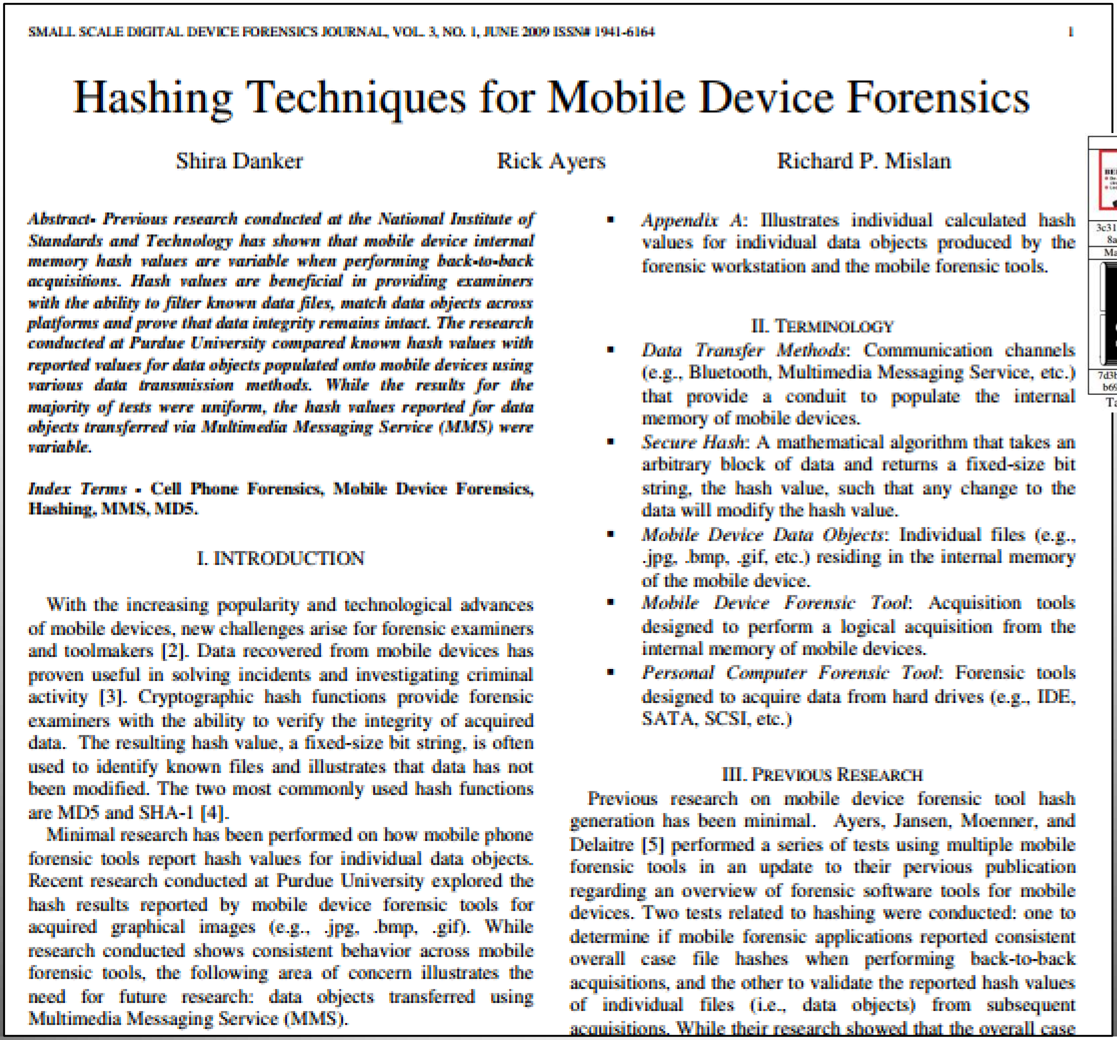
TECHNOLOGY has greatly changed the way criminals and investigators conduct business over the years. Criminals try to stay one step ahead of the law by adopting technology and using it as a means to conduct business quickly and quietly. Investigators are constantly pursuing offenders in an attempt to thwart their activities and it has turned into a game with both sides trying to learn the inner workings of new technology to work in their favor. In the past few years the market for Global Positioning Devices (GPS) has grown immensely and has become quite affordable to the average citizen. GPS units have diminished in size from the large clunky models first introduced to the public and now the technology is often a standard option on many other electronic

understanding of the algorithms and computations required to diagnose the location of a device, but one should be able to understand the principles and limitations of the design. The GPS system was developed by the United States Department of Defense as a tool for the military that could help soldiers navigate foreign territory and deliver munitions precisely on target. The satellite-based system was first employed in 1978 and now consists of a total of 24 satellites that continuously orbit the earth [1]. The system was strictly used for military operations initially, but the United States government opened up the service for civilian use in the 1980s. The signal supplied to the civilian sector suffered from Selective Availability (SA), which was an intentional degradation of the signal accuracy to make sure that adversaries of the country did not have the ability to mount attacks with the same precision as the United States. Selective Availability was turned off in 2000 by the United States and civilian receivers have gained a greater rate of accuracy since.

The satellite system is supported by a number of ground stations that monitor the data sent by the satellites and transmit corrective data back to the satellites [2]. As the satellites orbit the earth they send out two different radio signals designated L1 and L2. L1 is set aside for civilian use and transmits data that can be read by civilian receivers to determine location. These signals contain three pieces of information called ephemeris data, almanac data, and pseudorandom code. Ephemeris data contains the precise location of the satellite as well as the locations of all other satellites in the system.

GPS

National Institute of Standards and Technology
U.S. Department of Commerce



Hashing Techniques for Mobile Device Forensics

Shira Danker Rick Ayers Richard P. Mislan

Abstract- Previous research conducted at the National Institute of Standards and Technology has shown that mobile device internal memory hash values are variable when performing back-to-back acquisitions. Hash values are beneficial in providing examiners with the ability to filter known data files, match data objects across platforms and prove that data integrity remains intact. The research conducted at Purdue University compared known hash values with reported values for data objects populated onto mobile devices using various data transmission methods. While the results for the majority of tests were uniform, the hash values reported for data objects transferred via Multimedia Messaging Service (MMS) were variable.

***Index Terms* - Cell Phone Forensics, Mobile Device Forensics, Hashing, MMS, MD5.**

I. INTRODUCTION

With the increasing popularity and technological advances of mobile devices, new challenges arise for forensic examiners and toolmakers [2]. Data recovered from mobile devices has proven useful in solving incidents and investigating criminal activity [3]. Cryptographic hash functions provide forensic examiners with the ability to verify the integrity of acquired data. The resulting hash value, a fixed-size bit string, is often used to identify known files and illustrates that data has not been modified. The two most commonly used hash functions are MD5 and SHA-1 [4].

Minimal research has been performed on how mobile phone forensic tools report hash values for individual data objects. Recent research conducted at Purdue University explored the hash results reported by mobile device forensic tools for acquired graphical images (e.g., .jpg, .bmp, .gif). While research conducted shows consistent behavior across mobile forensic tools, the following area of concern illustrates the need for future research: data objects transferred using Multimedia Messaging Service (MMS).

- *Appendix A*: Illustrates individual calculated hash values for individual data objects produced by the forensic workstation and the mobile forensic tools.

II. TERMINOLOGY

- *Data Transfer Methods*: Communication channels (e.g., Bluetooth, Multimedia Messaging Service, etc.) that provide a conduit to populate the internal memory of mobile devices.
- *Secure Hash*: A mathematical algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the hash value, such that any change to the data will modify the hash value.
- *Mobile Device Data Objects*: Individual files (e.g., .jpg, .bmp, .gif, etc.) residing in the internal memory of the mobile device.
- *Mobile Device Forensic Tool*: Acquisition tools designed to perform a logical acquisition from the internal memory of mobile devices.
- *Personal Computer Forensic Tool*: Forensic tools designed to acquire data from hard drives (e.g., IDE, SATA, SCSI, etc.)

III. PREVIOUS RESEARCH

Previous research on mobile device forensic tool hash generation has been minimal. Ayers, Jansen, Moenner, and Delaitre [5] performed a series of tests using multiple mobile forensic tools in an update to their pervious publication regarding an overview of forensic software tools for mobile devices. Two tests related to hashing were conducted: one to determine if mobile forensic applications reported consistent overall case file hashes when performing back-to-back acquisitions, and the other to validate the reported hash values of individual files (i.e., data objects) from subsequent acquisitions. While their research showed that the overall case

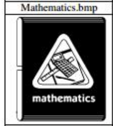
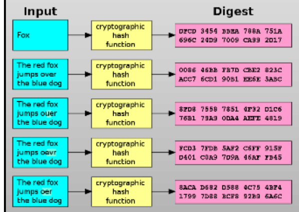
Test.jpg	Bluetooth.jpg	Card.jpg
3c3111ded5df821d66 8aecf9b598100b	6c8a1401a3af826450 4f16334e774b5c	77bebd7fb998797dd 5768c99fdbda8f6
Mathematics.bmp	Stress-test.gif	Mail.jpg
		
7d3b824769389bead b69b536a0295662	9b902382728b6bbdc 65009a5d1084041	d57fac85a5be5a7804 05a0484254256b

Table 1: Pre-define Data Set (Graphic Files) – MD5Sum



Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2017
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Hashing

National Institute of Standards and Technology
U.S. Department of Commerce

SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 1, NO. 1, JUNE 2007 1

Forensic Data Recovery from Flash Memory

Marcel Breeuwsma, Martien de Jongh, Coert Klaver, Ronald van der Kr

***Abstract*—Current forensic tools for examination of embedded systems like mobile phones and PDA's mostly perform data extraction on a logical level and do not consider the type of storage media during data analysis. This paper suggests a low level approach for the forensic examination of flash memories and describes three low-level data acquisition methods for making full memory copies of flash memory devices. Results are presented of a file system study in which USB memory sticks from 45 different make and models were used. For different mobile phones is shown how full memory copies of their flash memories can be made and which steps are needed to translate the extracted data into a format that can be understood by common forensic media analysis tools. Artifacts, caused by flash specific operations like block erasing and wear leveling, are discussed and directions are given for enhanced data recovery and analysis on data originating from flash memory.**

***Index Terms*—embedded systems, flash memory, physical analysis, hex analysis, forensic, mobile phones, USB sticks.**

I. Introduction

THE evolution in consumer electronics has caused an exponential growth in the amount of mobile digital data. The majority of mobile phones nowadays has a build in camera and is able to record, store, play and forward picture, audio, and video data. Some countries probably have more memory sticks than inhabitants. A lot of this data is related to human behavior and might become subject of a forensic investigation.

Flash memory is currently the most dominant non-volatile solid-state storage technology in consumer electronic products. An increasing number of embedded systems use high level file systems comparable to the file systems used on personal computers. Current forensic tools for examination of embedded systems like mobile phones or PDAs mostly perform logical data acquisition. With logical data acquisition it's often not possible to recover all data from a storage medium. Deleted data for example, but sometimes also other data which is not directly relevant from a user standpoint, can not be acquired and potentially interesting information might be missed. For this reason data acquisition is wanted at the lowest layer where

to file system level wher
tools can be used for fu
are given on data origin
phones. Chapter V expla
data originating from flas

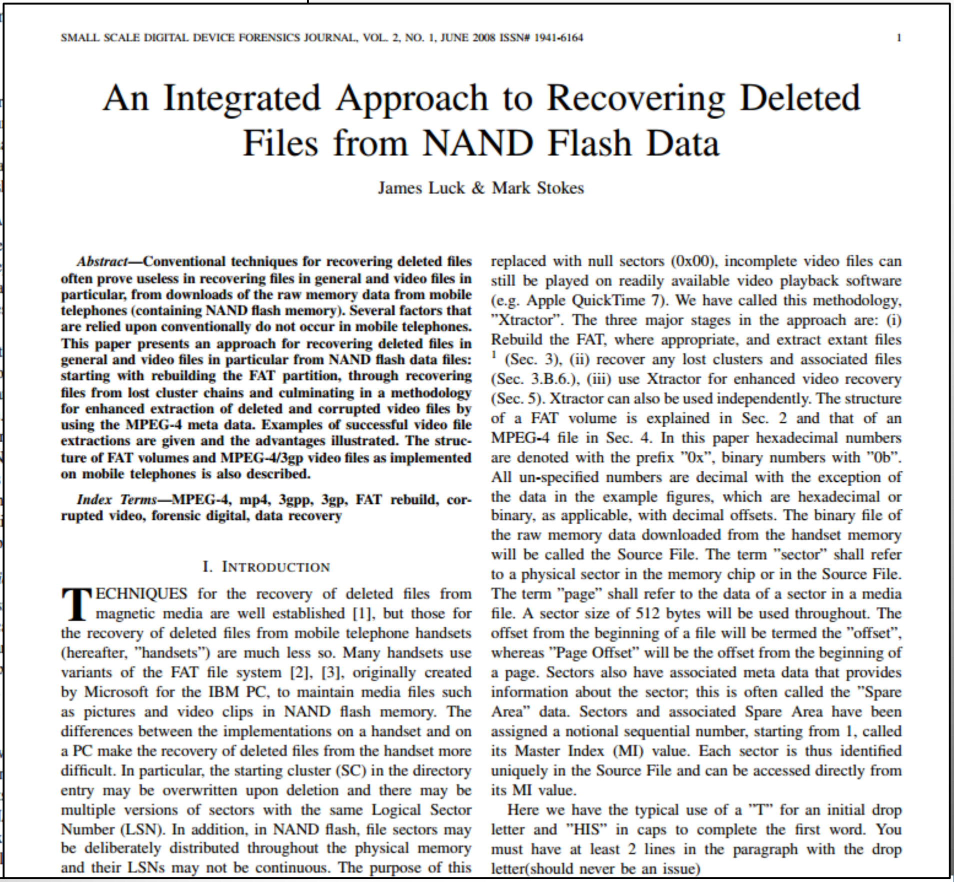
II. Fla

Flash memory is a type
electrically erased and re
in two flavors, NOR[1] fla
the basic logical structure
flash, NOR flash can be
which is the reason why it
of the flash memory is to
parts of NOR flash that a
used for user data storage.
disks, or multimedia centr
camera phones, use NAN
mobile data storage. This
technology first on the ph
perspective. An introducti
found in [5], more in dep

A. Physical Characteristi

The physical mechanis
based on storing electric
transistor. This charge ca
time without using an e
it will leak away caused
specifications for current
100 years.

Flash memory can be w
but it has to be erased in
re-written. Erasing result
completely with 1's. In N
further into pages, for ex
page is usually a multipl



SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 2, NO. 1, JUNE 2008 ISSN# 1941-6164 1

An Integrated Approach to Recovering Deleted Files from NAND Flash Data

James Luck & Mark Stokes

***Abstract*—Conventional techniques for recovering deleted files often prove useless in recovering files in general and video files in particular, from downloads of the raw memory data from mobile telephones (containing NAND flash memory). Several factors that are relied upon conventionally do not occur in mobile telephones. This paper presents an approach for recovering deleted files in general and video files in particular from NAND flash data files: starting with rebuilding the FAT partition, through recovering files from lost cluster chains and culminating in a methodology for enhanced extraction of deleted and corrupted video files by using the MPEG-4 meta data. Examples of successful video file extractions are given and the advantages illustrated. The structure of FAT volumes and MPEG-4/3gp video files as implemented on mobile telephones is also described.**

***Index Terms*—MPEG-4, mp4, 3gpp, 3gp, FAT rebuild, corrupted video, forensic digital, data recovery**

I. Introduction

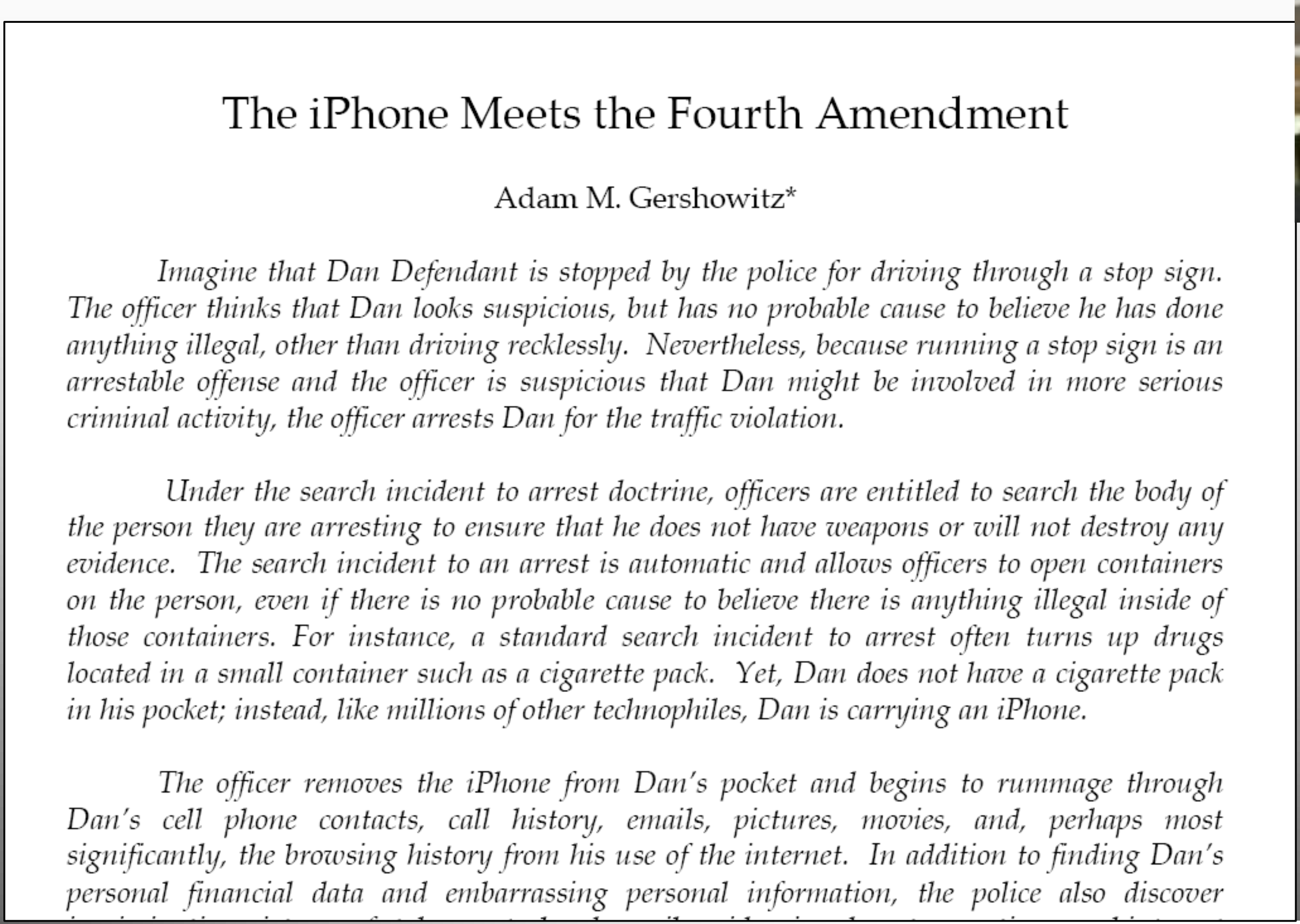
TECHNIQUES for the recovery of deleted files from magnetic media are well established [1], but those for the recovery of deleted files from mobile telephone handsets (hereafter, "handsets") are much less so. Many handsets use variants of the FAT file system [2], [3], originally created by Microsoft for the IBM PC, to maintain media files such as pictures and video clips in NAND flash memory. The differences between the implementations on a handset and on a PC make the recovery of deleted files from the handset more difficult. In particular, the starting cluster (SC) in the directory entry may be overwritten upon deletion and there may be multiple versions of sectors with the same Logical Sector Number (LSN). In addition, in NAND flash, file sectors may be deliberately distributed throughout the physical memory and their LSNs may not be continuous. The purpose of this replaced with null sectors (0x00), incomplete video files can still be played on readily available video playback software (e.g. Apple QuickTime 7). We have called this methodology, "Xtractor". The three major stages in the approach are: (i) Rebuild the FAT, where appropriate, and extract extant files [1] (Sec. 3), (ii) recover any lost clusters and associated files (Sec. 3.B.6.), (iii) use Xtractor for enhanced video recovery (Sec. 5). Xtractor can also be used independently. The structure of a FAT volume is explained in Sec. 2 and that of an MPEG-4 file in Sec. 4. In this paper hexadecimal numbers are denoted with the prefix "0x", binary numbers with "0b". All un-specified numbers are decimal with the exception of the data in the example figures, which are hexadecimal or binary, as applicable, with decimal offsets. The binary file of the raw memory data downloaded from the handset memory will be called the Source File. The term "sector" shall refer to a physical sector in the memory chip or in the Source File. The term "page" shall refer to the data of a sector in a media file. A sector size of 512 bytes will be used throughout. The offset from the beginning of a file will be termed the "offset", whereas "Page Offset" will be the offset from the beginning of a page. Sectors also have associated meta data that provides information about the sector; this is often called the "Spare Area" data. Sectors and associated Spare Area have been assigned a notional sequential number, starting from 1, called its Master Index (MI) value. Each sector is thus identified uniquely in the Source File and can be accessed directly from its MI value.

Here we have the typical use of a "T" for an initial drop letter and "HIS" in caps to complete the first word. You must have at least 2 lines in the paragraph with the drop letter(should never be an issue)

Images/Videos

National Institute of Standards and Technology
U.S. Department of Commerce

Legal



The iPhone Meets the Fourth Amendment

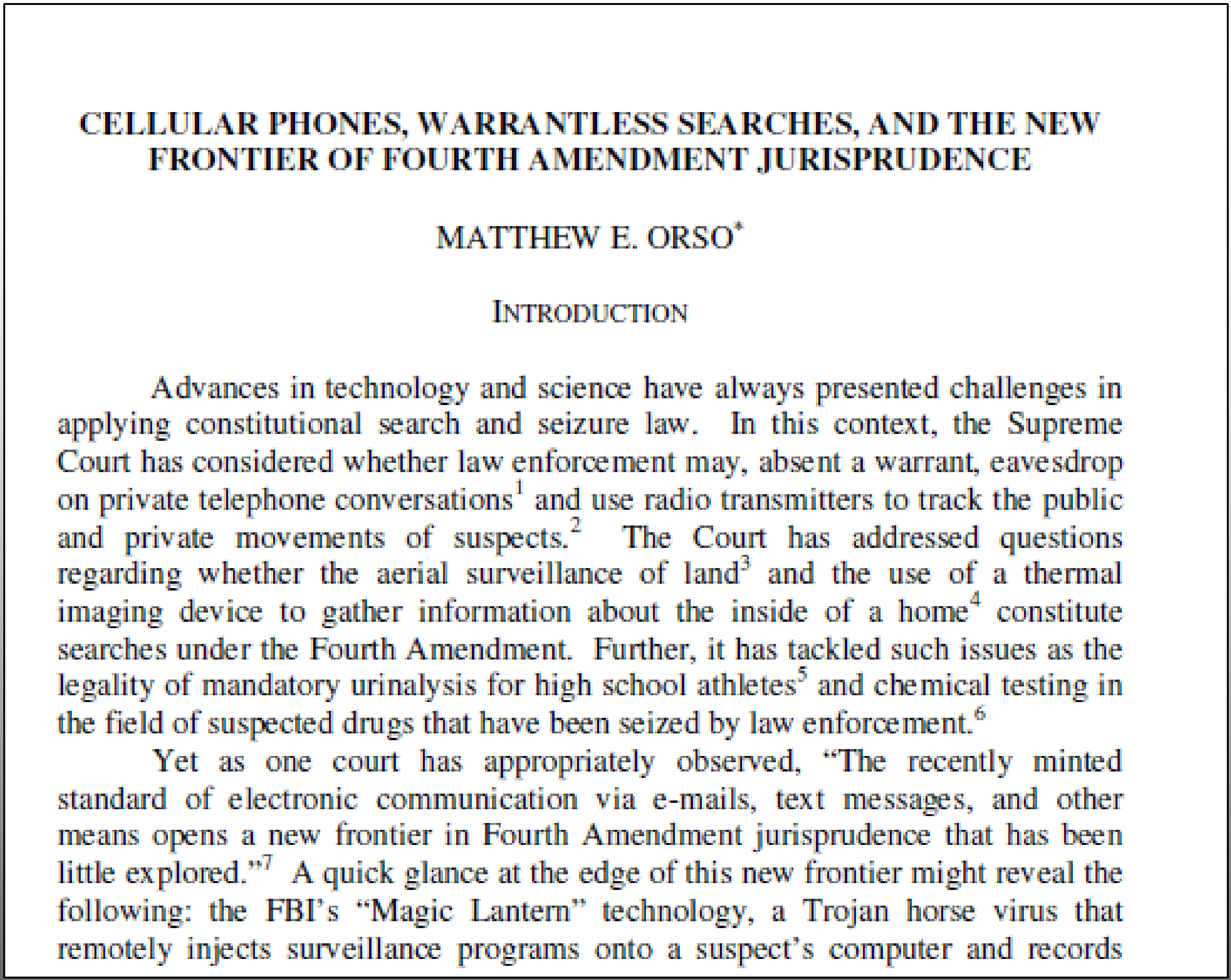
Adam M. Gershowitz*

Imagine that Dan Defendant is stopped by the police for driving through a stop sign. The officer thinks that Dan looks suspicious, but has no probable cause to believe he has done anything illegal, other than driving recklessly. Nevertheless, because running a stop sign is an arrestable offense and the officer is suspicious that Dan might be involved in more serious criminal activity, the officer arrests Dan for the traffic violation.

Under the search incident to arrest doctrine, officers are entitled to search the body of the person they are arresting to ensure that he does not have weapons or will not destroy any evidence. The search incident to an arrest is automatic and allows officers to open containers on the person, even if there is no probable cause to believe there is anything illegal inside of those containers. For instance, a standard search incident to arrest often turns up drugs located in a small container such as a cigarette pack. Yet, Dan does not have a cigarette pack in his pocket; instead, like millions of other technophiles, Dan is carrying an iPhone.

The officer removes the iPhone from Dan's pocket and begins to rummage through Dan's cell phone contacts, call history, emails, pictures, movies, and, perhaps most significantly, the browsing history from his use of the internet. In addition to finding Dan's personal financial data and embarrassing personal information, the police also discover

National Institute of Standards and Technology
U.S. Department of Commerce



CELLULAR PHONES, WARRANTLESS SEARCHES, AND THE NEW FRONTIER OF FOURTH AMENDMENT JURISPRUDENCE

MATTHEW E. ORSO[*]

INTRODUCTION

Advances in technology and science have always presented challenges in applying constitutional search and seizure law. In this context, the Supreme Court has considered whether law enforcement may, absent a warrant, eavesdrop on private telephone conversations[1] and use radio transmitters to track the public and private movements of suspects.[2] The Court has addressed questions regarding whether the aerial surveillance of land[3] and the use of a thermal imaging device to gather information about the inside of a home[4] constitute searches under the Fourth Amendment. Further, it has tackled such issues as the legality of mandatory urinalysis for high school athletes[5] and chemical testing in the field of suspected drugs that have been seized by law enforcement.[6]

Yet as one court has appropriately observed, "The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored."[7] A quick glance at the edge of this new frontier might reveal the following: the FBI's "Magic Lantern" technology, a Trojan horse virus that remotely injects surveillance programs onto a suspect's computer and records

Legal

National Institute of Standards and Technology
U.S. Department of Commerce

Operating Systems

SYNGRESS

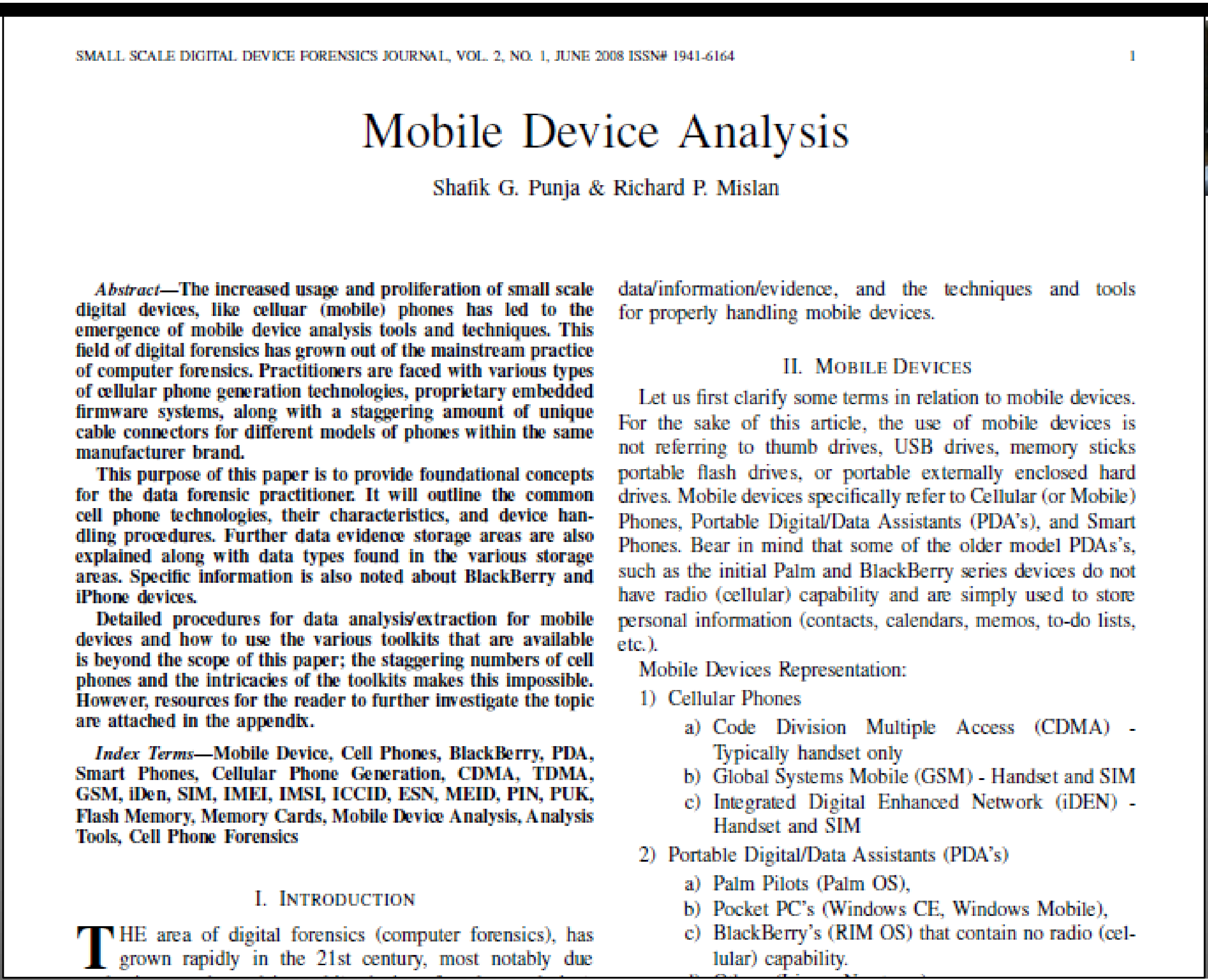
ANDROID FORENSICS

Investigation, Analysis and Mobile Security for Google Android

Andrew Hoog

Android

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Mobile Device Analysis

Shafik G. Punja & Richard P. Mislan

***Abstract*—The increased usage and proliferation of small scale digital devices, like celluar (mobile) phones has led to the emergence of mobile device analysis tools and techniques. This field of digital forensics has grown out of the mainstream practice of computer forensics. Practitioners are faced with various types of cellular phone generation technologies, proprietary embedded firmware systems, along with a staggering amount of unique cable connectors for different models of phones within the same manufacturer brand.**

This purpose of this paper is to provide foundational concepts for the data forensic practitioner. It will outline the common cell phone technologies, their characteristics, and device handling procedures. Further data evidence storage areas are also explained along with data types found in the various storage areas. Specific information is also noted about BlackBerry and iPhone devices.

Detailed procedures for data analysis/extraction for mobile devices and how to use the various toolkits that are available is beyond the scope of this paper; the staggering numbers of cell phones and the intricacies of the toolkits makes this impossible. However, resources for the reader to further investigate the topic are attached in the appendix.

***Index Terms*—Mobile Device, Cell Phones, BlackBerry, PDA, Smart Phones, Cellular Phone Generation, CDMA, TDMA, GSM, iDen, SIM, IMEI, IMSI, ICCID, ESN, MEID, PIN, PUK, Flash Memory, Memory Cards, Mobile Device Analysis, Analysis Tools, Cell Phone Forensics**

I. Introduction

THE area of digital forensics (computer forensics), has grown rapidly in the 21st century, most notably due

data/information/evidence, and the techniques and tools for properly handling mobile devices.

II. Mobile Devices

Let us first clarify some terms in relation to mobile devices. For the sake of this article, the use of mobile devices is not referring to thumb drives, USB drives, memory sticks portable flash drives, or portable externally enclosed hard drives. Mobile devices specifically refer to Cellular (or Mobile) Phones, Portable Digital/Data Assistants (PDA's), and Smart Phones. Bear in mind that some of the older model PDAs's, such as the initial Palm and BlackBerry series devices do not have radio (cellular) capability and are simply used to store personal information (contacts, calendars, memos, to-do lists, etc.).

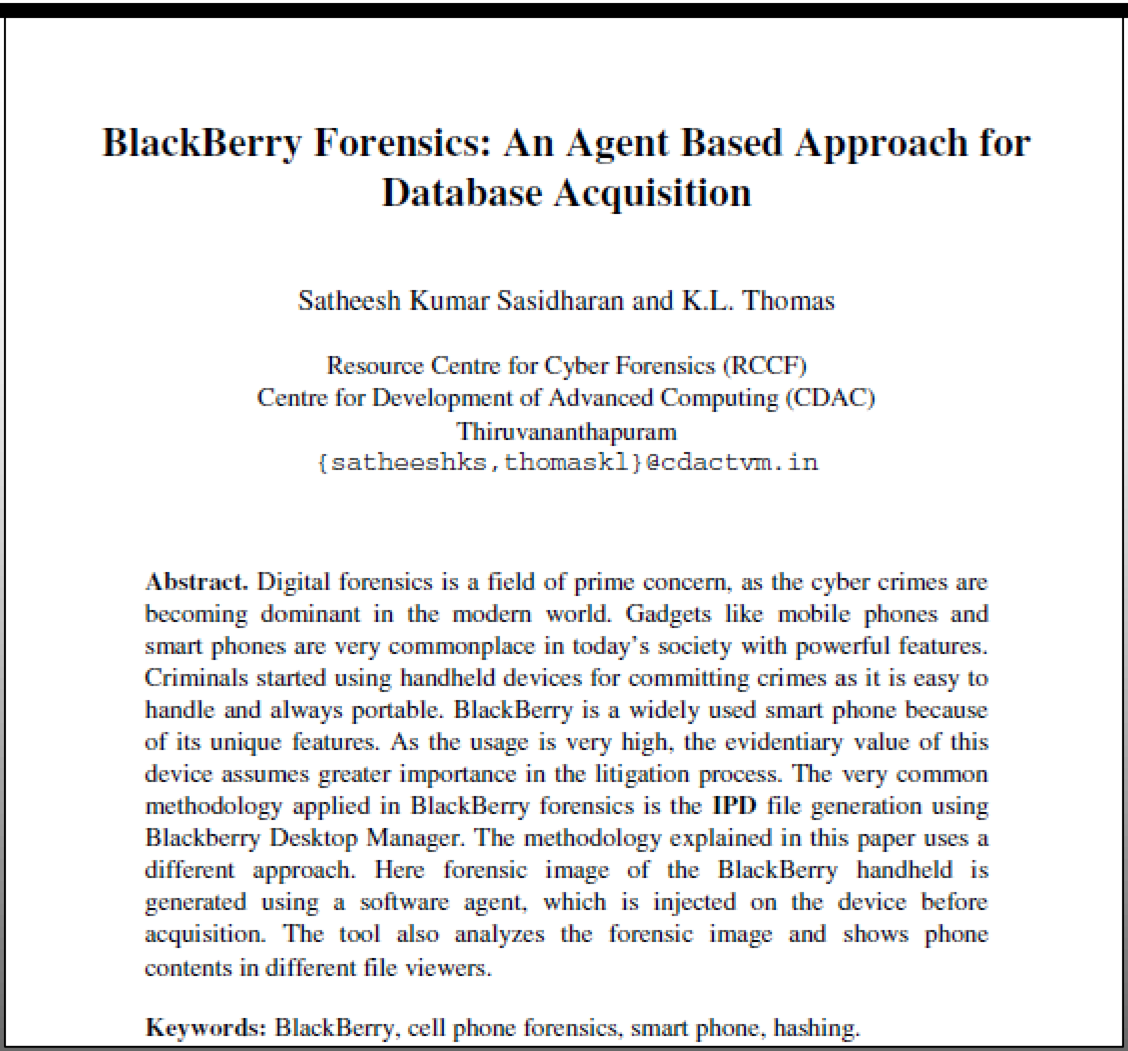
Mobile Devices Representation:

1) Cellular Phones
   a) Code Division Multiple Access (CDMA) - Typically handset only
   b) Global Systems Mobile (GSM) - Handset and SIM
   c) Integrated Digital Enhanced Network (iDEN) - Handset and SIM
2) Portable Digital/Data Assistants (PDA's)
   a) Palm Pilots (Palm OS),
   b) Pocket PC's (Windows CE, Windows Mobile),
   c) BlackBerry's (RIM OS) that contain no radio (cellular) capability.

BlackBerry

National Institute of Standards and Technology
U.S. Department of Commerce

BlackBerry



BlackBerry Forensics: An Agent Based Approach for Database Acquisition

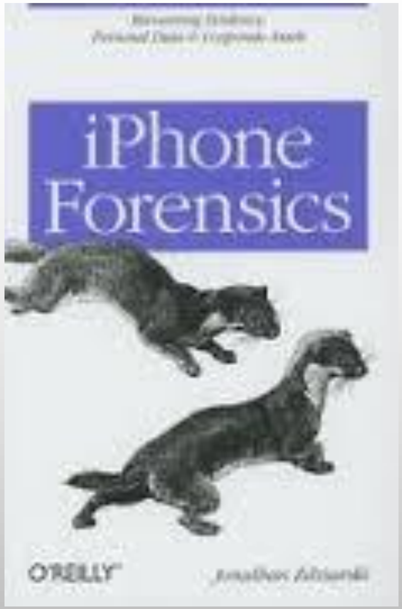
Satheesh Kumar Sasidharan and K.L. Thomas

Resource Centre for Cyber Forensics (RCCF)
Centre for Development of Advanced Computing (CDAC)
Thiruvananthapuram
{satheeshks,thomaskl}@cdactvm.in

Abstract. Digital forensics is a field of prime concern, as the cyber crimes are becoming dominant in the modern world. Gadgets like mobile phones and smart phones are very commonplace in today's society with powerful features. Criminals started using handheld devices for committing crimes as it is easy to handle and always portable. BlackBerry is a widely used smart phone because of its unique features. As the usage is very high, the evidentiary value of this device assumes greater importance in the litigation process. The very common methodology applied in BlackBerry forensics is the **IPD** file generation using Blackberry Desktop Manager. The methodology explained in this paper uses a different approach. Here forensic image of the BlackBerry handheld is generated using a software agent, which is injected on the device before acquisition. The tool also analyzes the forensic image and shows phone contents in different file viewers.

Keywords: BlackBerry, cell phone forensics, smart phone, hashing.

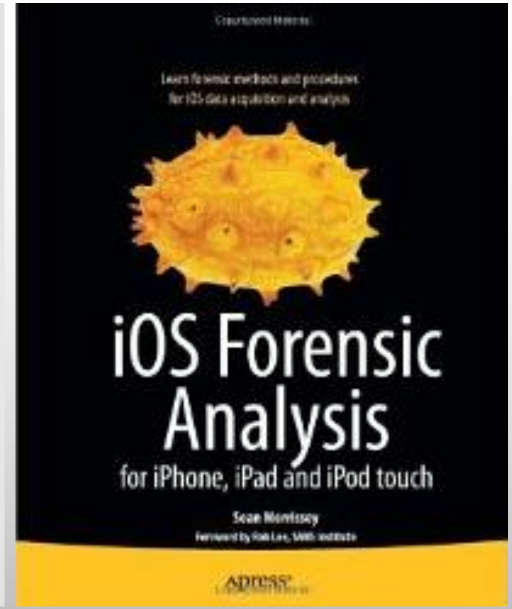
iOS


Recovering Evidence,
Personal Data & Corporate Assets

iPhone Forensics

O'REILLY

Jonathan Zdziarski


Copyrighted Material

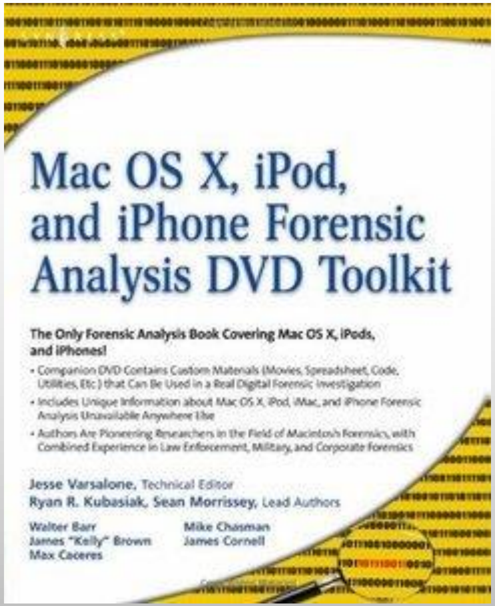
Learn forensic methods and procedures
for iOS data acquisition and analysis

iOS Forensic Analysis
for iPhone, iPad and iPod touch

Sean Morrissey

Foreword by Rob Lee, SANS Institute

Apress®


Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit

The Only Forensic Analysis Book Covering Mac OS X, iPods, and iPhones!

- Companion DVD Contains Custom Materials (Movies, Spreadsheet, Code, Utilities, Etc.) that Can Be Used in a Real Digital Forensic Investigation
- Includes Unique Information about Mac OS X, iPod, iMac, and iPhone Forensic Analysis Unavailable Anywhere Else
- Authors Are Pioneering Researchers in the Field of Macintosh Forensics, with Combined Experience in Law Enforcement, Military, and Corporate Forensics

Jesse Varsalone, Technical Editor
Ryan R. Kubasiak, Sean Morrissey, Lead Authors

Walter Barr
James "Kelly" Brown
Max Caceres

Mike Chasman
James Cornell

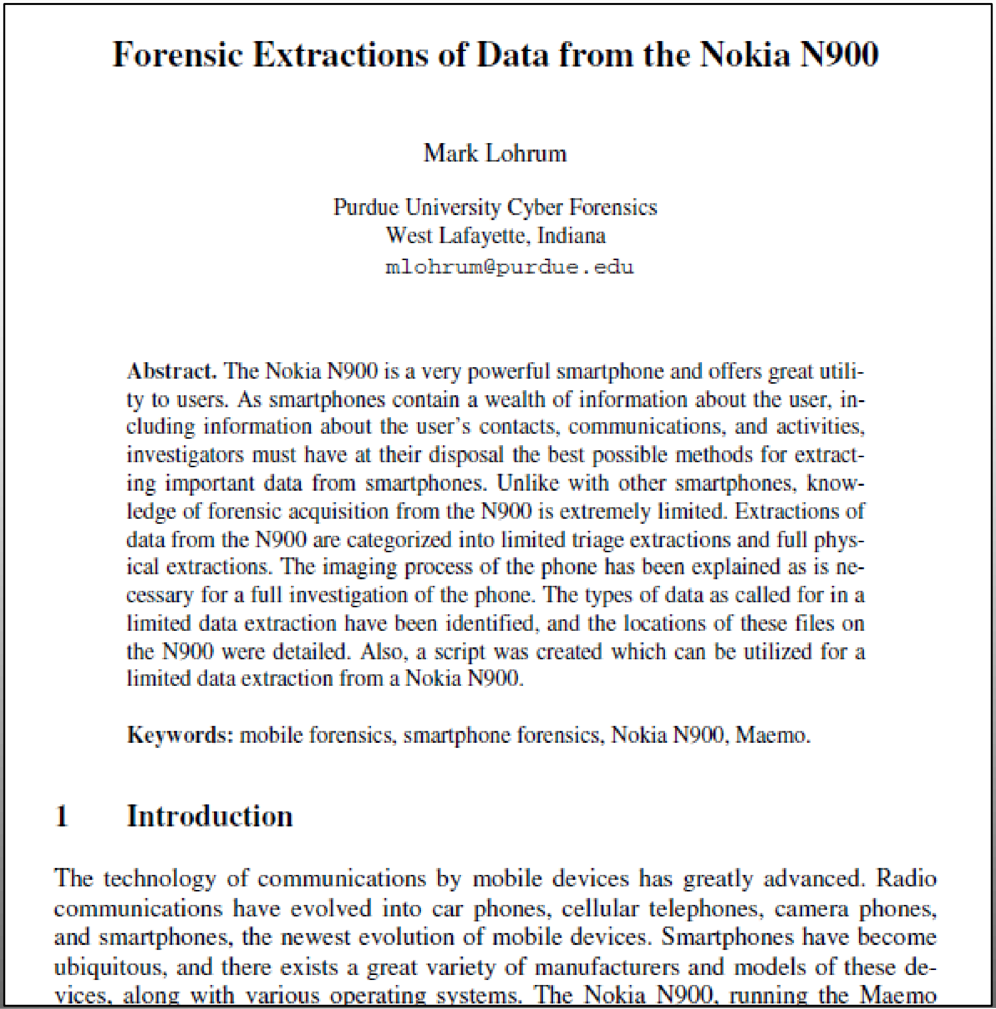
Jonathan Zdziarski

Sean Morrisey

Ryan Kubasiak

National Institute of Standards and Technology
U.S. Department of Commerce

Maemo



Forensic Extractions of Data from the Nokia N900

Mark Lohrum

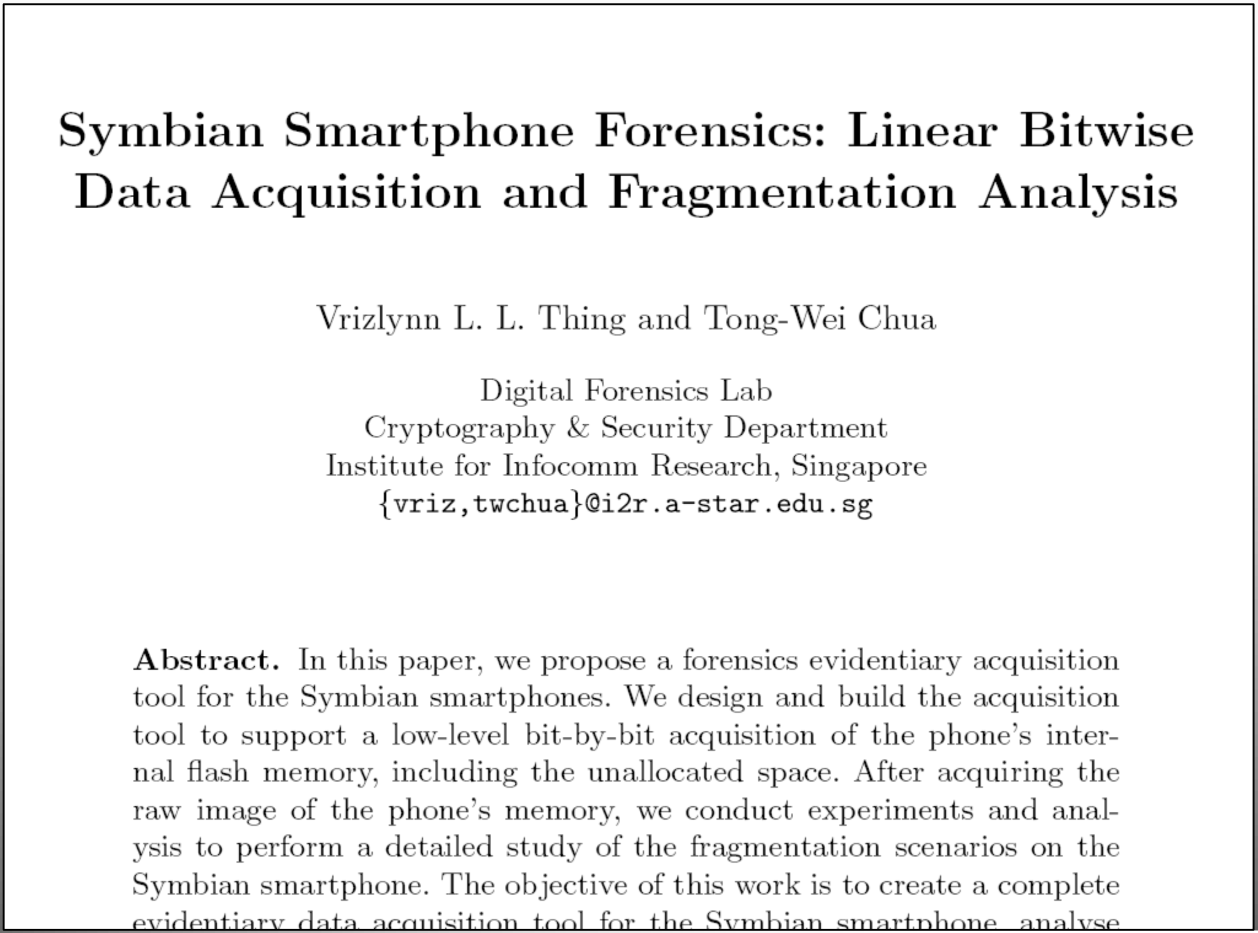
Purdue University Cyber Forensics
West Lafayette, Indiana
mlohrum@purdue.edu

Abstract. The Nokia N900 is a very powerful smartphone and offers great utility to users. As smartphones contain a wealth of information about the user, including information about the user's contacts, communications, and activities, investigators must have at their disposal the best possible methods for extracting important data from smartphones. Unlike with other smartphones, knowledge of forensic acquisition from the N900 is extremely limited. Extractions of data from the N900 are categorized into limited triage extractions and full physical extractions. The imaging process of the phone has been explained as is necessary for a full investigation of the phone. The types of data as called for in a limited data extraction have been identified, and the locations of these files on the N900 were detailed. Also, a script was created which can be utilized for a limited data extraction from a Nokia N900.

Keywords: mobile forensics, smartphone forensics, Nokia N900, Maemo.

1 Introduction

The technology of communications by mobile devices has greatly advanced. Radio communications have evolved into car phones, cellular telephones, camera phones, and smartphones, the newest evolution of mobile devices. Smartphones have become ubiquitous, and there exists a great variety of manufacturers and models of these devices, along with various operating systems. The Nokia N900, running the Maemo



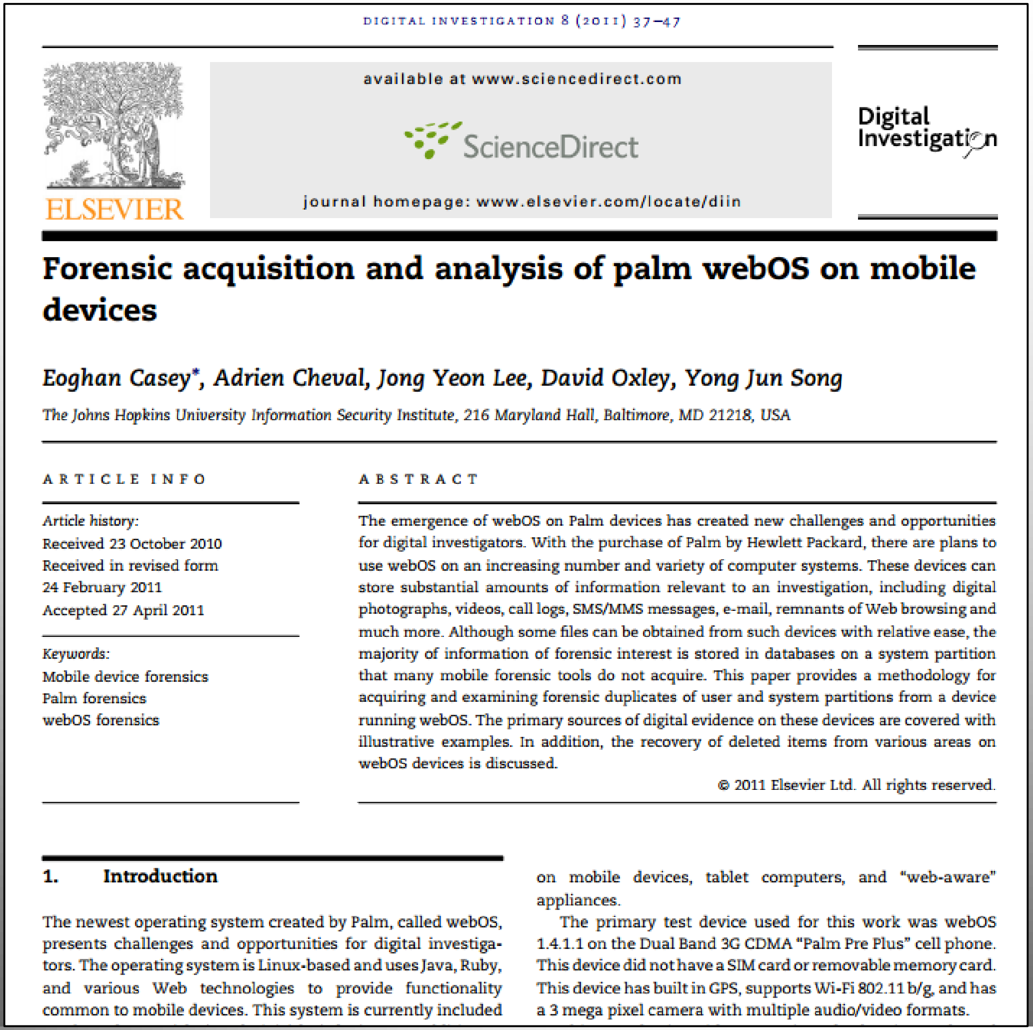
Symbian Smartphone Forensics: Linear Bitwise Data Acquisition and Fragmentation Analysis

Vrizlynn L. L. Thing and Tong-Wei Chua

Digital Forensics Lab
Cryptography & Security Department
Institute for Infocomm Research, Singapore
{vriz,twchua}@i2r.a-star.edu.sg

Abstract. In this paper, we propose a forensics evidentiary acquisition tool for the Symbian smartphones. We design and build the acquisition tool to support a low-level bit-by-bit acquisition of the phone's internal flash memory, including the unallocated space. After acquiring the raw image of the phone's memory, we conduct experiments and analysis to perform a detailed study of the fragmentation scenarios on the Symbian smartphone. The objective of this work is to create a complete evidentiary data acquisition tool for the Symbian smartphone, analyse

Symbian



DIGITAL INVESTIGATION 8 (2011) 37–47

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

ELSEVIER

Digital Investigation

Forensic acquisition and analysis of palm webOS on mobile devices

Eoghan Casey, Adrien Cheval, Jong Yeon Lee, David Oxley, Yong Jun Song*

The Johns Hopkins University Information Security Institute, 216 Maryland Hall, Baltimore, MD 21218, USA

ARTICLE INFO

Article history:
Received 23 October 2010
Received in revised form
24 February 2011
Accepted 27 April 2011

Keywords:
Mobile device forensics
Palm forensics
webOS forensics

ABSTRACT

The emergence of webOS on Palm devices has created new challenges and opportunities for digital investigators. With the purchase of Palm by Hewlett Packard, there are plans to use webOS on an increasing number and variety of computer systems. These devices can store substantial amounts of information relevant to an investigation, including digital photographs, videos, call logs, SMS/MMS messages, e-mail, remnants of Web browsing and much more. Although some files can be obtained from such devices with relative ease, the majority of information of forensic interest is stored in databases on a system partition that many mobile forensic tools do not acquire. This paper provides a methodology for acquiring and examining forensic duplicates of user and system partitions from a device running webOS. The primary sources of digital evidence on these devices are covered with illustrative examples. In addition, the recovery of deleted items from various areas on webOS devices is discussed.

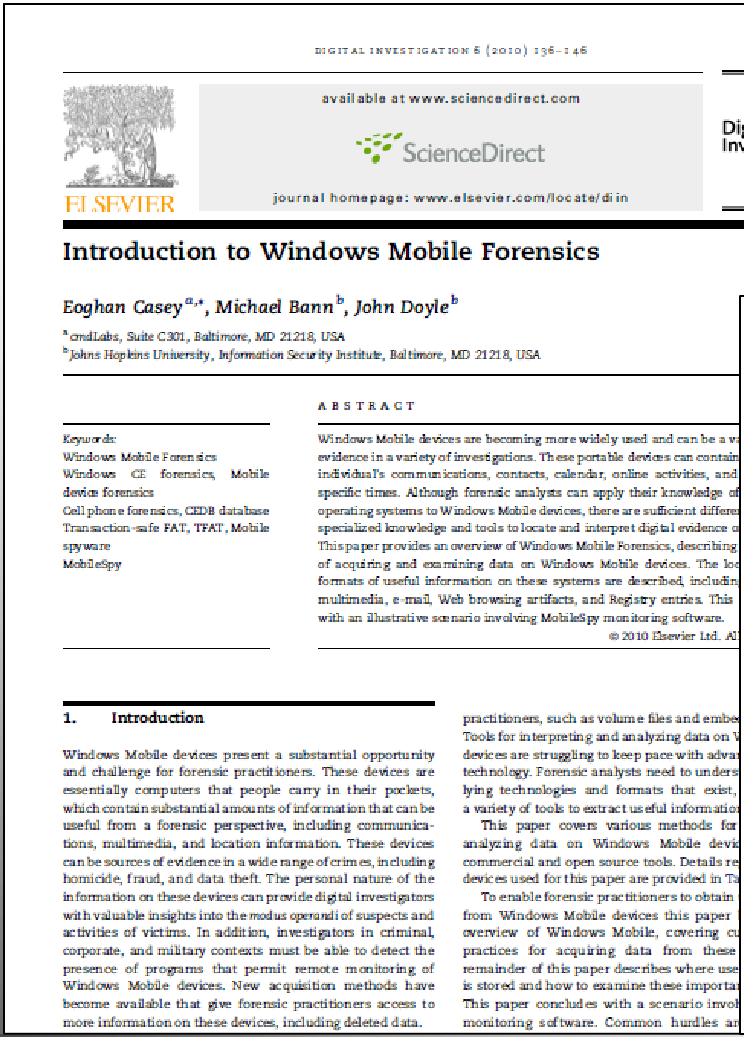
1. Introduction

The newest operating system created by Palm, called webOS, presents challenges and opportunities for digital investigators. The operating system is Linux-based and uses Java, Ruby, and various Web technologies to provide functionality common to mobile devices. This system is currently included on mobile devices, tablet computers, and "web-aware" appliances.

The primary test device used for this work was webOS 1.4.1.1 on the Dual Band 3G CDMA "Palm Pre Plus" cell phone. This device did not have a SIM card or removable memory card. This device has built in GPS, supports Wi-Fi 802.11 b/g, and has a 3 mega pixel camera with multiple audio/video formats.

WebOS

National Institute of Standards and Technology
U.S. Department of Commerce



DIGITAL INVESTIGATION 6 (2010) 136–146

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

ELSEVIER

Digital Investigation

Introduction to Windows Mobile Forensics

Eoghan Casey[a,*], Michael Bann[b], John Doyle[b]

[a] cmdLabs, Suite C301, Baltimore, MD 21218, USA
[b] Johns Hopkins University, Information Security Institute, Baltimore, MD 21218, USA

ABSTRACT

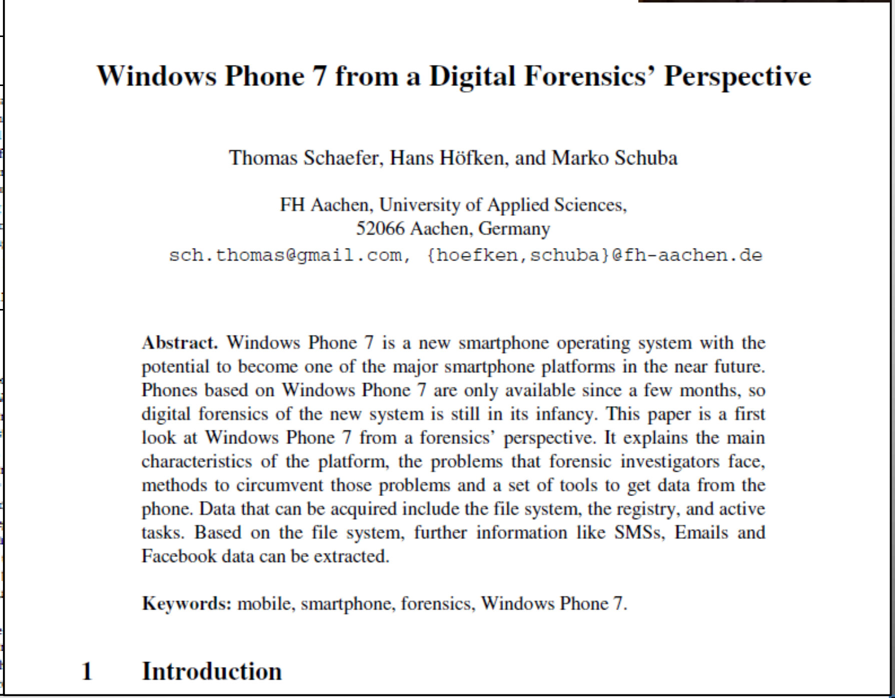
Keywords:
Windows Mobile Forensics
Windows CE forensics, Mobile device forensics
Cell phone forensics, CEDB database
Transaction-safe FAT, TFAT, Mobile spyware
MobileSpy

Windows Mobile devices are becoming more widely used and can be a va
evidence in a variety of investigations. These portable devices can contain
individual's communications, contacts, calendar, online activities, and
specific times. Although forensic analysts can apply their knowledge of
operating systems to Windows Mobile devices, there are sufficient differe
specialized knowledge and tools to locate and interpret digital evidence o
This paper provides an overview of Windows Mobile Forensics, describing
of acquiring and examining data on Windows Mobile devices. The loc
formats of useful information on these systems are described, includin
multimedia, e-mail, Web browsing artifacts, and Registry entries. This
with an illustrative scenario involving MobileSpy monitoring software.
© 2010 Elsevier Ltd. All

1. Introduction

Windows Mobile devices present a substantial opportunity and challenge for forensic practitioners. These devices are essentially computers that people carry in their pockets, which contain substantial amounts of information that can be useful from a forensic perspective, including communications, multimedia, and location information. These devices can be sources of evidence in a wide range of crimes, including homicide, fraud, and data theft. The personal nature of the information on these devices can provide digital investigators with valuable insights into the *modus operandi* of suspects and activities of victims. In addition, investigators in criminal, corporate, and military contexts must be able to detect the presence of programs that permit remote monitoring of Windows Mobile devices. New acquisition methods have become available that give forensic practitioners access to more information on these devices, including deleted data.

practitioners, such as volume files and embe
Tools for interpreting and analyzing data on W
devices are struggling to keep pace with advan
technology. Forensic analysts need to unders
lying technologies and formats that exist,
a variety of tools to extract useful informatio
This paper covers various methods for
analyzing data on Windows Mobile devic
commercial and open source tools. Details re
devices used for this paper are provided in Ta
To enable forensic practitioners to obtain
from Windows Mobile devices this paper
overview of Windows Mobile, covering cu
practices for acquiring data from these
remainder of this paper describes where use
is stored and how to examine these importa
This paper concludes with a scenario invol
monitoring software. Common hurdles ar



Windows Phone 7 from a Digital Forensics' Perspective

Thomas Schaefer, Hans Höfken, and Marko Schuba

FH Aachen, University of Applied Sciences,
52066 Aachen, Germany
sch.thomas@gmail.com, {hoefken,schuba}@fh-aachen.de

Abstract. Windows Phone 7 is a new smartphone operating system with the potential to become one of the major smartphone platforms in the near future. Phones based on Windows Phone 7 are only available since a few months, so digital forensics of the new system is still in its infancy. This paper is a first look at Windows Phone 7 from a forensics' perspective. It explains the main characteristics of the platform, the problems that forensic investigators face, methods to circumvent those problems and a set of tools to get data from the phone. Data that can be acquired include the file system, the registry, and active tasks. Based on the file system, further information like SMSs, Emails and Facebook data can be extracted.

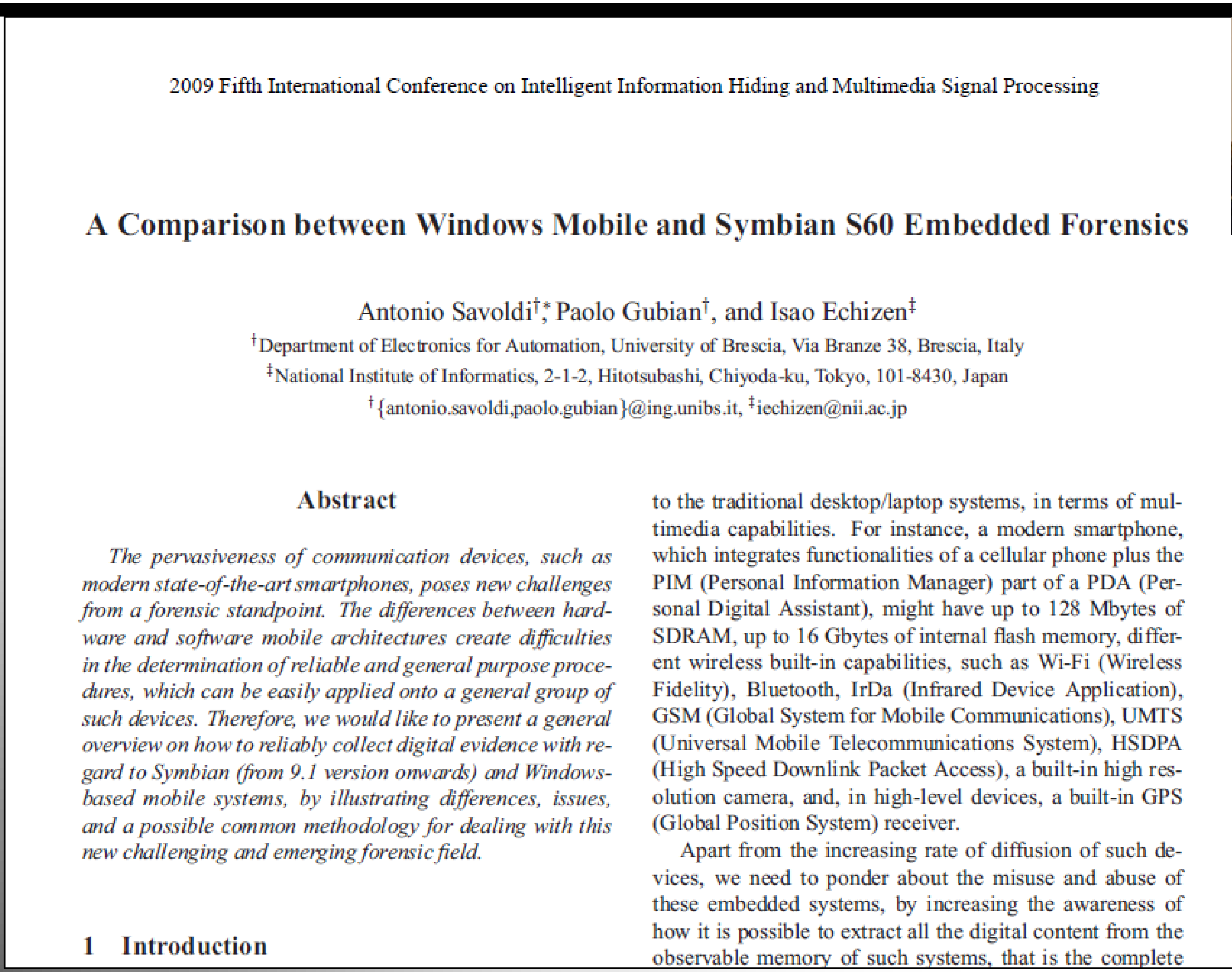
Keywords: mobile, smartphone, forensics, Windows Phone 7.

1 Introduction

Windows

National Institute of Standards and Technology
U.S. Department of Commerce

Comparing OS's



2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

A Comparison between Windows Mobile and Symbian S60 Embedded Forensics

Antonio Savoldi[†,*], Paolo Gubian[†], and Isao Echizen[‡]

[†]Department of Electronics for Automation, University of Brescia, Via Branze 38, Brescia, Italy

[‡]National Institute of Informatics, 2-1-2, Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430, Japan

[†]{antonio.savoldi,paolo.gubian}@ing.unibs.it, [‡]iechizen@nii.ac.jp

Abstract

The pervasiveness of communication devices, such as modern state-of-the-art smartphones, poses new challenges from a forensic standpoint. The differences between hardware and software mobile architectures create difficulties in the determination of reliable and general purpose procedures, which can be easily applied onto a general group of such devices. Therefore, we would like to present a general overview on how to reliably collect digital evidence with regard to Symbian (from 9.1 version onwards) and Windows-based mobile systems, by illustrating differences, issues, and a possible common methodology for dealing with this new challenging and emerging forensic field.

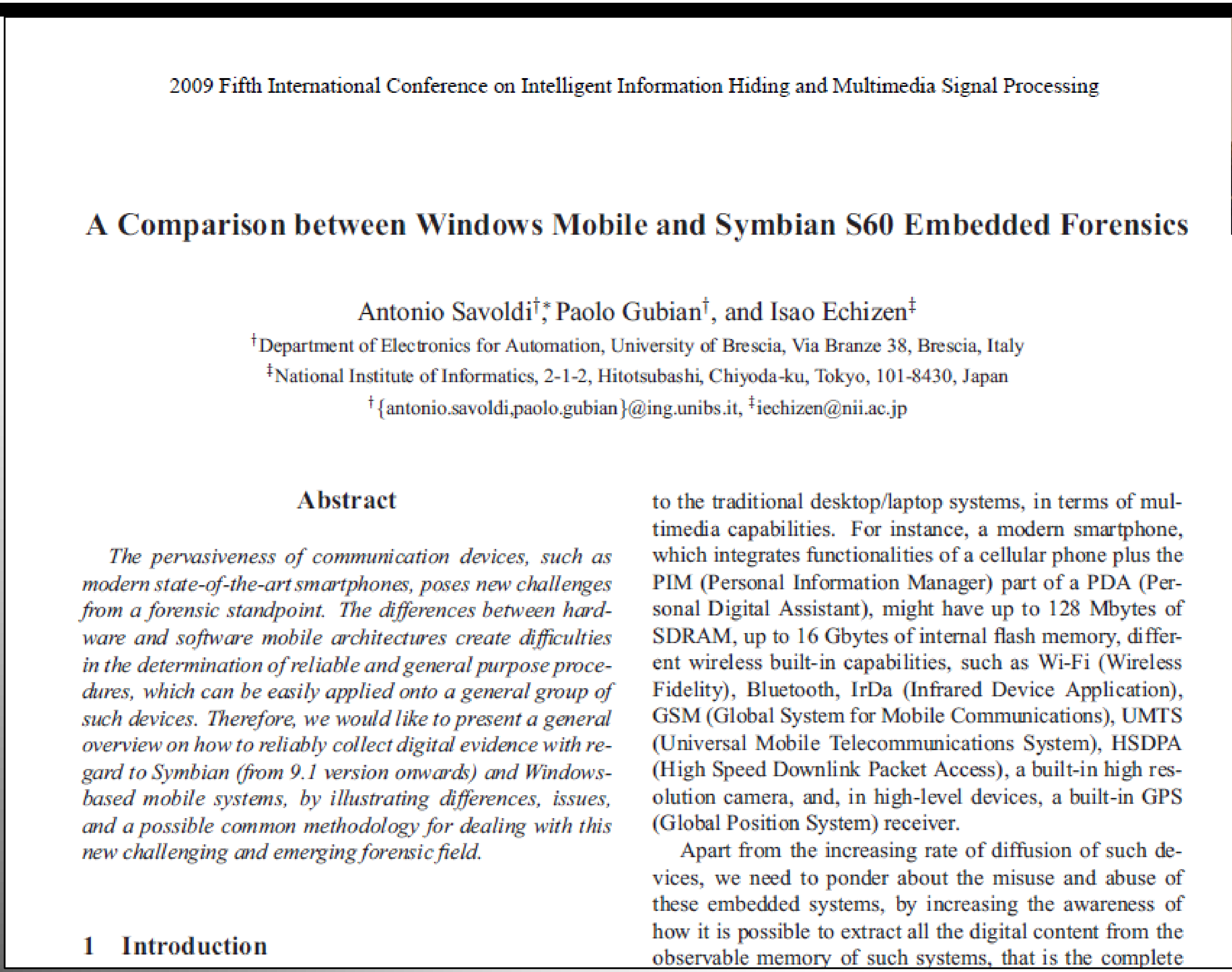
1 Introduction

to the traditional desktop/laptop systems, in terms of multimedia capabilities. For instance, a modern smartphone, which integrates functionalities of a cellular phone plus the PIM (Personal Information Manager) part of a PDA (Personal Digital Assistant), might have up to 128 Mbytes of SDRAM, up to 16 Gbytes of internal flash memory, different wireless built-in capabilities, such as Wi-Fi (Wireless Fidelity), Bluetooth, IrDa (Infrared Device Application), GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System), HSDPA (High Speed Downlink Packet Access), a built-in high resolution camera, and, in high-level devices, a built-in GPS (Global Position System) receiver.

Apart from the increasing rate of diffusion of such devices, we need to ponder about the misuse and abuse of these embedded systems, by increasing the awareness of how it is possible to extract all the digital content from the observable memory of such systems, that is the complete

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Comparing OS's



2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

A Comparison between Windows Mobile and Symbian S60 Embedded Forensics

Antonio Savoldi[†],[*] Paolo Gubian[†], and Isao Echizen[‡]
[†]Department of Electronics for Automation, University of Brescia, Via Branze 38, Brescia, Italy
[‡]National Institute of Informatics, 2-1-2, Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430, Japan
[†]{antonio.savoldi,paolo.gubian}@ing.unibs.it, [‡]iechizen@nii.ac.jp

Abstract

The pervasiveness of communication devices, such as modern state-of-the-art smartphones, poses new challenges from a forensic standpoint. The differences between hardware and software mobile architectures create difficulties in the determination of reliable and general purpose procedures, which can be easily applied onto a general group of such devices. Therefore, we would like to present a general overview on how to reliably collect digital evidence with regard to Symbian (from 9.1 version onwards) and Windows-based mobile systems, by illustrating differences, issues, and a possible common methodology for dealing with this new challenging and emerging forensic field.

1 Introduction

to the traditional desktop/laptop systems, in terms of multimedia capabilities. For instance, a modern smartphone, which integrates functionalities of a cellular phone plus the PIM (Personal Information Manager) part of a PDA (Personal Digital Assistant), might have up to 128 Mbytes of SDRAM, up to 16 Gbytes of internal flash memory, different wireless built-in capabilities, such as Wi-Fi (Wireless Fidelity), Bluetooth, IrDa (Infrared Device Application), GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System), HSDPA (High Speed Downlink Packet Access), a built-in high resolution camera, and, in high-level devices, a built-in GPS (Global Position System) receiver.

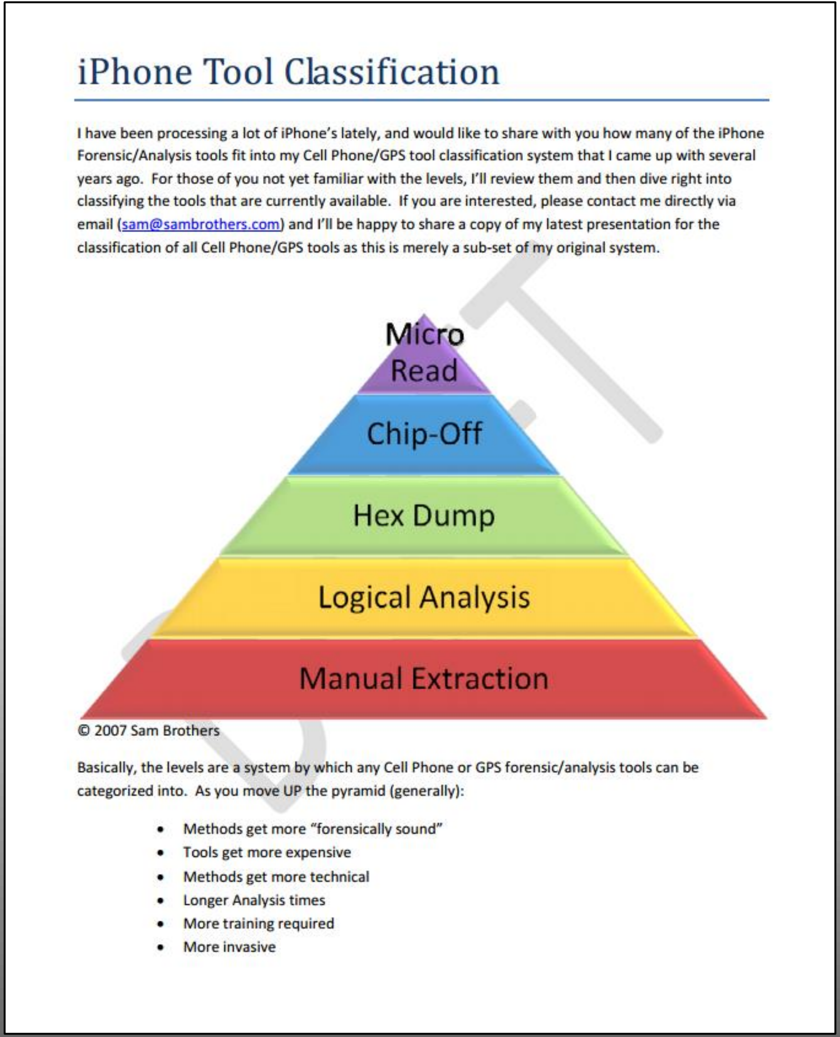
Apart from the increasing rate of diffusion of such devices, we need to ponder about the misuse and abuse of these embedded systems, by increasing the awareness of how it is possible to extract all the digital content from the observable memory of such systems, that is the complete

National Institute of Standards and Technology
U.S. Department of Commerce

and a few others worth mentioning…

Not found in the Journals…

Levels of Forensics



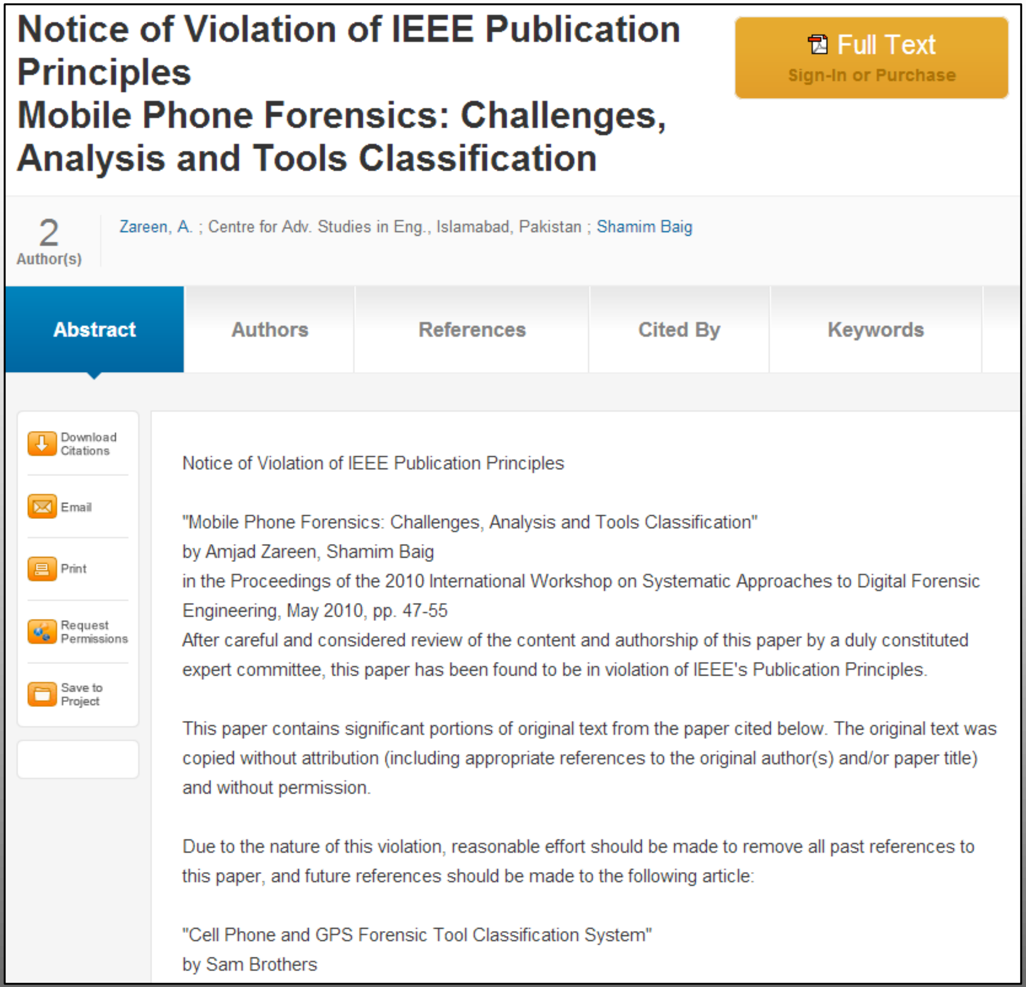
iPhone Tool Classification

I have been processing a lot of iPhone's lately, and would like to share with you how many of the iPhone Forensic/Analysis tools fit into my Cell Phone/GPS tool classification system that I came up with several years ago. For those of you not yet familiar with the levels, I'll review them and then dive right into classifying the tools that are currently available. If you are interested, please contact me directly via email (sam@sambrothers.com) and I'll be happy to share a copy of my latest presentation for the classification of all Cell Phone/GPS tools as this is merely a sub-set of my original system.

© 2007 Sam Brothers

Basically, the levels are a system by which any Cell Phone or GPS forensic/analysis tools can be categorized into. As you move UP the pyramid (generally):

- Methods get more "forensically sound"
- Tools get more expensive
- Methods get more technical
- Longer Analysis times
- More training required
- More invasive



Notice of Violation of IEEE Publication Principles
Mobile Phone Forensics: Challenges, Analysis and Tools Classification

2 Author(s)
Zareen, A. ; Centre for Adv. Studies in Eng., Islamabad, Pakistan ; Shamim Baig

Notice of Violation of IEEE Publication Principles

"Mobile Phone Forensics: Challenges, Analysis and Tools Classification"
by Amjad Zareen, Shamim Baig
in the Proceedings of the 2010 International Workshop on Systematic Approaches to Digital Forensic Engineering, May 2010, pp. 47-55
After careful and considered review of the content and authorship of this paper by a duly constituted expert committee, this paper has been found to be in violation of IEEE's Publication Principles.

This paper contains significant portions of original text from the paper cited below. The original text was copied without attribution (including appropriate references to the original author(s) and/or paper title) and without permission.

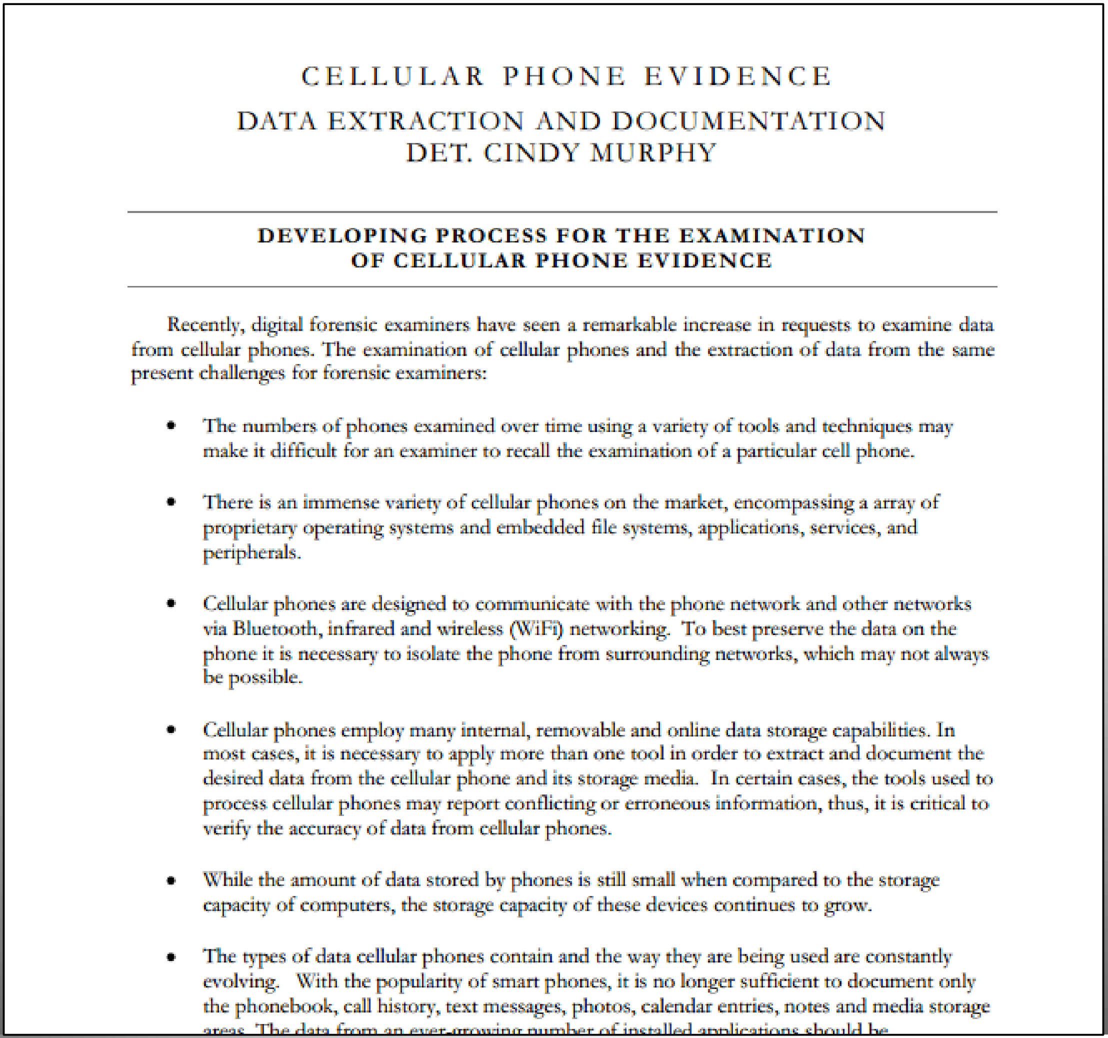
Due to the nature of this violation, reasonable effort should be made to remove all past references to this paper, and future references should be made to the following article:

"Cell Phone and GPS Forensic Tool Classification System"
by Sam Brothers

Levels of Forensics

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Process for Examination



CELLULAR PHONE EVIDENCE

DATA EXTRACTION AND DOCUMENTATION
DET. CINDY MURPHY

DEVELOPING PROCESS FOR THE EXAMINATION OF CELLULAR PHONE EVIDENCE

Recently, digital forensic examiners have seen a remarkable increase in requests to examine data from cellular phones. The examination of cellular phones and the extraction of data from the same present challenges for forensic examiners:

- The numbers of phones examined over time using a variety of tools and techniques may make it difficult for an examiner to recall the examination of a particular cell phone.

- There is an immense variety of cellular phones on the market, encompassing a array of proprietary operating systems and embedded file systems, applications, services, and peripherals.

- Cellular phones are designed to communicate with the phone network and other networks via Bluetooth, infrared and wireless (WiFi) networking. To best preserve the data on the phone it is necessary to isolate the phone from surrounding networks, which may not always be possible.

- Cellular phones employ many internal, removable and online data storage capabilities. In most cases, it is necessary to apply more than one tool in order to extract and document the desired data from the cellular phone and its storage media. In certain cases, the tools used to process cellular phones may report conflicting or erroneous information, thus, it is critical to verify the accuracy of data from cellular phones.

- While the amount of data stored by phones is still small when compared to the storage capacity of computers, the storage capacity of these devices continues to grow.

- The types of data cellular phones contain and the way they are being used are constantly evolving. With the popularity of smart phones, it is no longer sufficient to document only the phonebook, call history, text messages, photos, calendar entries, notes and media storage areas. The data from an ever-growing number of installed applications should be

National Institute of Standards and Technology
U.S. Department of Commerce

CHIP-OFF AND JTAG ANALYSIS FOR MOBILE DEVICE FORENSICS

Written by Bob Elder

IN THE FIELD of mobile-device forensics, the practices of "chip-off" and "JTAG" analysis have become topics of growing interest among the community. As mobile devices continue to bring new challenges to the examiner, these two disciplines warrant close attention, as they both offer examiners avenues for deeper data access, the ability to bypass lock codes, and a way to recover data from damaged devices.

While today's commercial tools continue to provide innovations at an impressive rate and offer extensive and expanding phone support with increasing data-recovery abilities, the unfortunate reality is that there is a seemingly infinite number of devices that continue to challenge examiners, creating the requirement for alternative means of data recovery.

While the use of chip-off and JTAG can be very useful for data recovery, it is imperative that examiners understand the risks involved before making attempts on devices...especially when it comes to evidence.

Ultimately, the goal for the mobile-device forensic examiner is to obtain a physical image of the memory chip from mobile devices. And while today such bit-by-bit acquisition support from the commercial tools is increasing, in many instances such a physical dump cannot be accomplished without direct access to the memory chip.

Additionally, for devices that are damaged or locked with an encryption scheme that is beyond today's tools' abilities to bypass or crack, the chip-off and JTAG methods are among the alternative solutions for examiners looking to gain access to the memory.

In a perfect world, the commercial tools would do it all, and the examiner could process easily and comprehensively the mounting piles of mobile devices in their lab. Unfortunately, the reality is we don't live on the set of *CSI: Miami*—and as anyone who has spent any time trying to acquire data from mobile devices knows, the general rule remains: you just never know what you will be confronted with next, and just how much data can be obtained. Further, considering that commercial tools most often connect to the device through a USB connection, some device manufacturers employ memory management schemes that inhibit the data transfer through the communication port via controllers that make it impossible to acquire a complete image of the memory. Simply put, chip-off or JTAG techniques are the only way to obtain a complete image on some devices.

This article aims to introduce the chip-off and JTAG techniques for the mobile-device forensic examiner and provide the basics for those who are looking to learn more.

Introduction to chip-off and JTAG

The *chip-off* technique describes the practice of removing a memory chip, or any chip, from a circuit board and reading it. The chips are often tested and programmed with the "JTAG" method. The term *JTAG* (Joint Test Action Group) is the original acronym and name of an IEEE group that set the standards for what would become the 1149.1 Standard Test Access Port and Boundary-Scan Architecture. In plain English, the group established a universally accepted means for testing wire-line interconnects on printed circuit boards. Today, the ports are used for testing integrated circuits, and they are the common test and debug interface for mobile devices and digital products.

These are not new concepts by themselves, and have in fact been in practice for several years in the integrated circuit (IC) programming and testing fields. However, a byproduct of both of these low-level access techniques is the ability to acquire raw data from the memory chip. For the mobile-device examiner, these practices offer another way to access and acquire the raw data from the memory chip.

Chip-off and JTAG techniques are opening new avenues for the mobile-device examiner to recover data. There have been more than a few instances where old mobile phones in evidence archives that were thought to be inaccessible are being examined again, this time successfully.

Prior to engaging in the practice of chip-off or JTAG efforts for mobile-device forensics, a solid understanding of key characteristics of the mobile device's structure is necessary to properly and successfully pursue these techniques. Particularly, the examiner must have a familiarity with modern mobile-devices' configurations, the memory types, how they manage data internally, where memory chips are located, and how to identify JTAG connectors on the mot mobile device. Buildi foundation of knowlec and how data is storec essential for the exam down the chip-off or J

This is an Android HTC mobile phone that is wired up for the JTAG process.

Additionally, a soli the skills for repair, di chip removal is crucia pursue these techniqu

In our mobile-devi chip-off and JTAG cla ners at Wild PCS teac to properly identify the components of a mobile device, disassemble and reassemble components, as well as how to properly remove and prepare the memory chips for reading. This is in addition to the education on how to repair a broken device to make it operational and examinable with today's forensic tools. These hands-on skills are essential to anyone who is looking to recover data using chip-off or JTAG techniques.

Chip-off and JTAG are as far from push-button forensics as one can get, and examiners intent on pursuing these practices have to be educated, prepared, and very patient.

While not covered in this article, readers are strongly encouraged to learn and understand the following concepts:

❑ NAND Memory (TSOP and BGA)

❑ NOR Memory

❑ Volatile RAM

❑ Flash Translation Layer—Controller Chips

❑ Wear Leveling—Garbage Collection

Similarities and Differences Between Chip-Off and JTAG Forensics

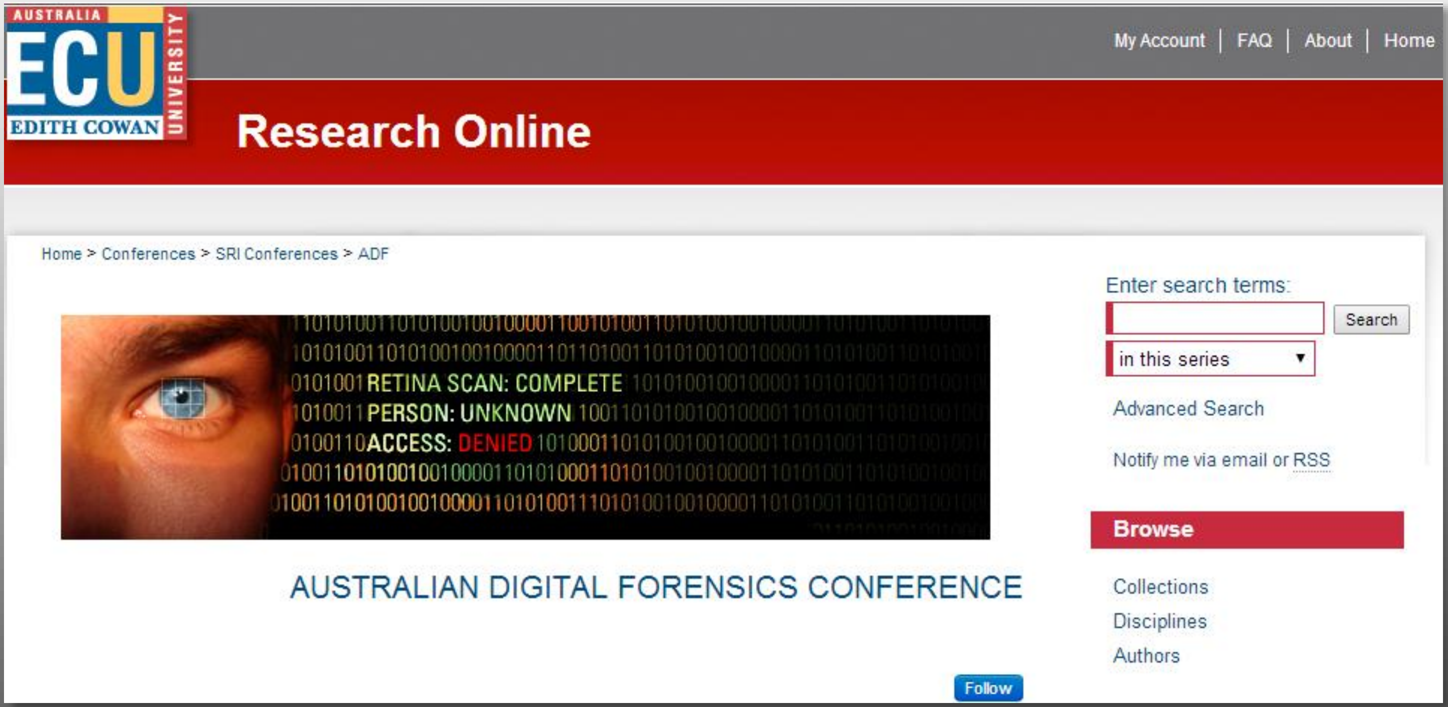
Initially, the major difference between chip-off and JTAG is that the chip-off technique is a more destructive method; once a memory chip is removed from a mobile device, it cannot be returned to the original mobile device. It follows, of course, that once a memory chip is removed from a mobile device, the device cannot be returned to normal operation or examined using a commercial tool. When a device is damaged beyond repair, but the memory chip is intact, the chip-off technique is

JTAG

National Institute of Standards and Technology
U.S. Department of Commerce

Academic Journals and Conferences

Australian Digital Forensics Conference – Edith Cowan University



Home > Conferences > SRI Conferences > ADF

Enter search terms:

AUSTRALIAN DIGITAL FORENSICS CONFERENCE

http://ro.ecu.edu.au/adf/

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

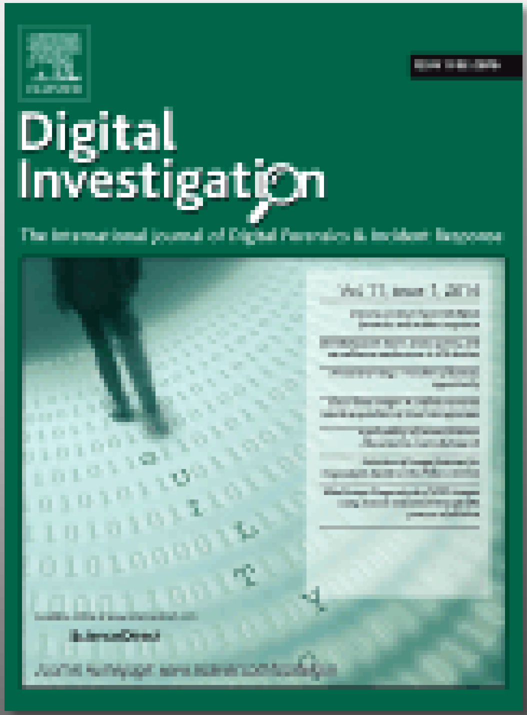
Digital Forensic Reasearch Work Shop

DFRWS

http://www.dfrws.org/2014/cfp.shtml

National Institute of Standards and Technology
U.S. Department of Commerce

Digital Investigation



Digital Investigation

The International Journal of Digital Forensics & Incident Response

Vol 11, Issue 1, 2014

ScienceDirect

http://www.journals.elsevier.com/digital-investigation/

Hawaii International Conference on Systems Sciences

2014 47th Hawaii International Conference on System Science

Android Anti-forensics: Modifying CyanogenMod

Karl-Johan Karlsson
University of Glasgow
creideiki@lysator.liu.se

William Bradley Glisson
University of South Alabama
bglisson@southalabama.edu

Abstract

Mobile devices implementing Android operating systems inherently create opportunities to present environments that are conducive to anti-forensic activities. Previous mobile forensics research focused on applications and data hiding anti-forensics solutions. In this work, a set of modifications were developed and implemented on a CyanogenMod community distribution of the Android operating system. The execution of these solutions successfully prevented data extractions, blocked the installation of forensic tools, created extraction delays and presented false data to industry accepted forensic analysis tools without impacting normal use of the device. The research contribution is an initial empirical analysis of the viability of operating system modifications in an anti-forensics context along with providing the foundation for future research.

1. Introduction

The increasing integration of mobile smartphones, in today's digitally dependant, highly networked, communication based societies creates an component analysis, an analyst would start by disassembling the phone and removing the surface mounted memory chips, which is a delicate and highly risky procedure. The memory chips can be read by standardized readers, but the interpretation of the data depends on the software running on the phone. A much easier method is to let the phone run, and access the data through the normal interfaces provided by the software. However, this presents a high risk of data being modified, both as a normal function of the phone and/or by specialized anti-forensic applications. The savings in time and effort gained by the utilization of normal interfaces are substantial enough that this technique is endorsed by the Association of Chief Police Officers (ACPO) [32] and the American National Institute of Standards and Technology [24].

Due to this acceptance, forensic analysts rely heavily on the correct functioning of the phone's software when performing analyses. Hence, altering functionality is a way of thwarting an analysis. Smartphones running operating systems such as Android and iOS are designed to allow the installation of third-party applications. This has allowed for the development of applications with anti-forensic functionality [7, 12, 27]. However, these

http://www.hicss.hawaii.edu/

National Institute of Standards and Technology
U.S. Department of Commerce

International Conference on Digital Forensics an Cyber Crime

ICDF2C

Digital Forensics & Cyber Crime

http://d-forensics.org/2014/show/home

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

International Journal of Digital Crime and Forensics

An official publication of the Information Resources Management Association

INTERNATIONAL JOURNAL OF

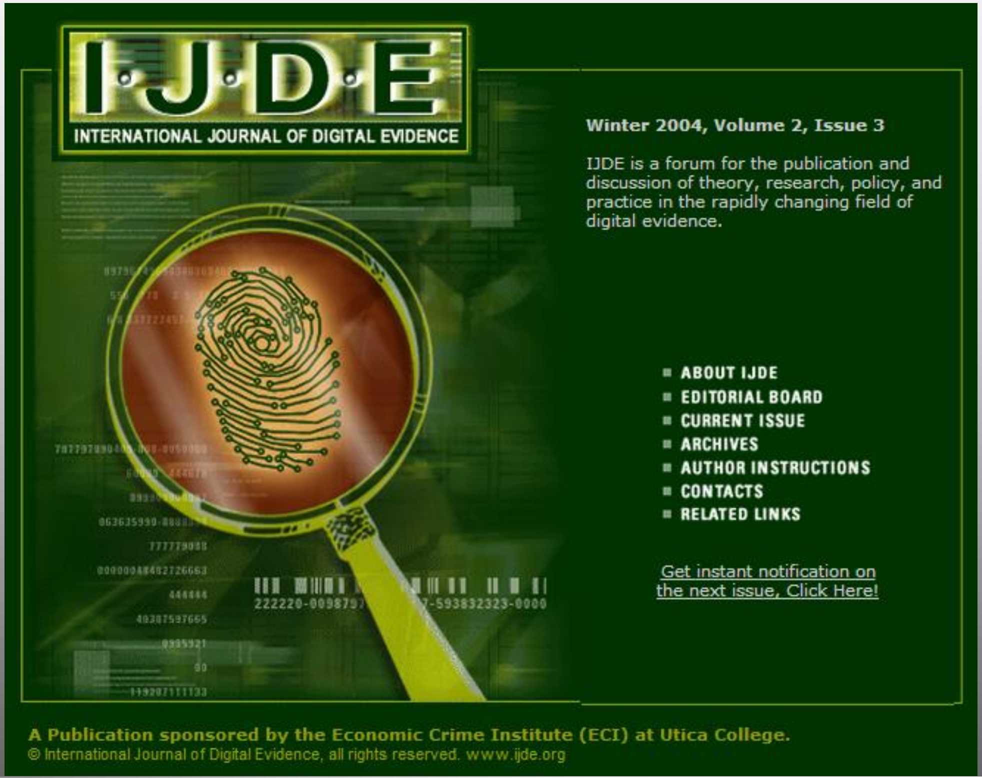
Digital Crime and Forensics

IGI PUBLISHING

Publisher of IT books, journals and cases since 1988
www.igi-global.com

http://www.igi-global.com/journal/international-journal-digital-crime-forensics/1112

International Journal of Digital Evidence



Winter 2004, Volume 2, Issue 3

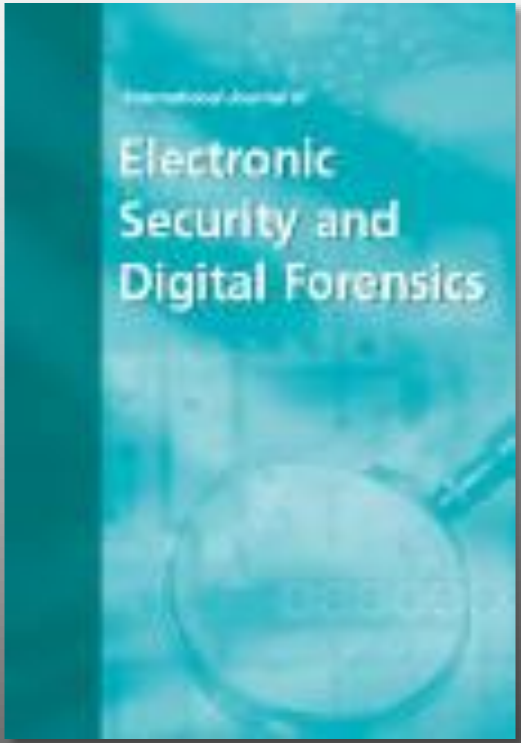
IJDE is a forum for the publication and discussion of theory, research, policy, and practice in the rapidly changing field of digital evidence.

Get instant notification on the next issue, Click Here!

A Publication sponsored by the Economic Crime Institute (ECI) at Utica College.

Archive.org – IJDE.org

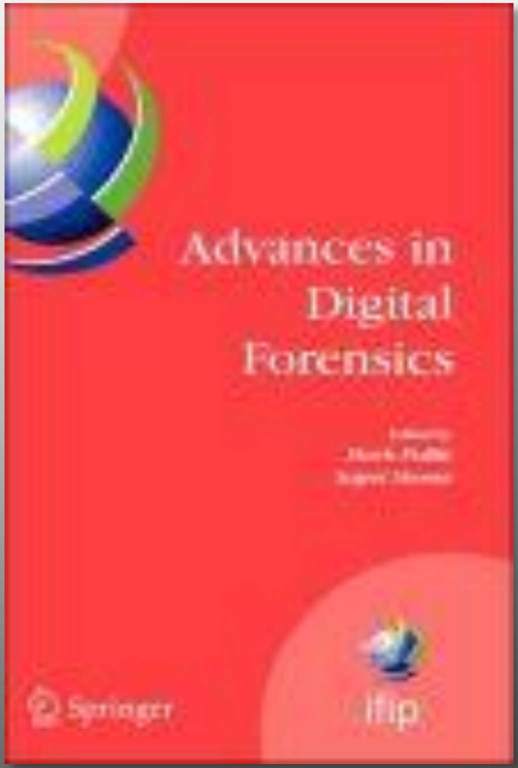
International Journal of Electronic Security and Digital Forensics



http://www.inderscience.com/jhome.php?jcode=ijesdf

National Institute of Standards and Technology
U.S. Department of Commerce

International Federation for Inform Processing



Advances in Digital Forensics

[illegible]

Springer

ifip

http://www.ifip.org/

Journal of Digital Forensic Practice

DIGITAL
FORENSIC
PRACTICE

http://www.tandfonline.com/toc/udfp20/current#.U588efldWac

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

The Journal of Digital Forensics, Security and Law

JDFSL

The Journal of Digital Forensics, Security and Law

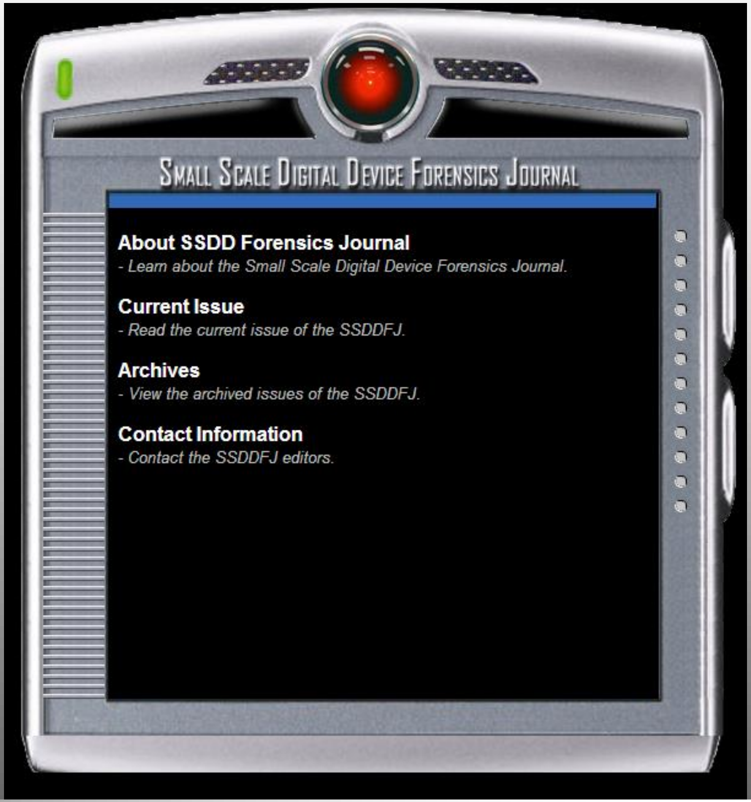
WINTER 2006

http://www.adfsl.org/journal.htm

NIST

National Institute of Standards and Technology
U.S. Department of Commerce

Small Scale Digital Device Forensics Journal



About SSDD Forensics Journal
- Learn about the Small Scale Digital Device Forensics Journal.

Current Issue
- Read the current issue of the SSDDFJ.

Archives
- View the archived issues of the SSDDFJ.

Contact Information
- Contact the SSDDFJ editors.

http://www.ssddfj.org

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

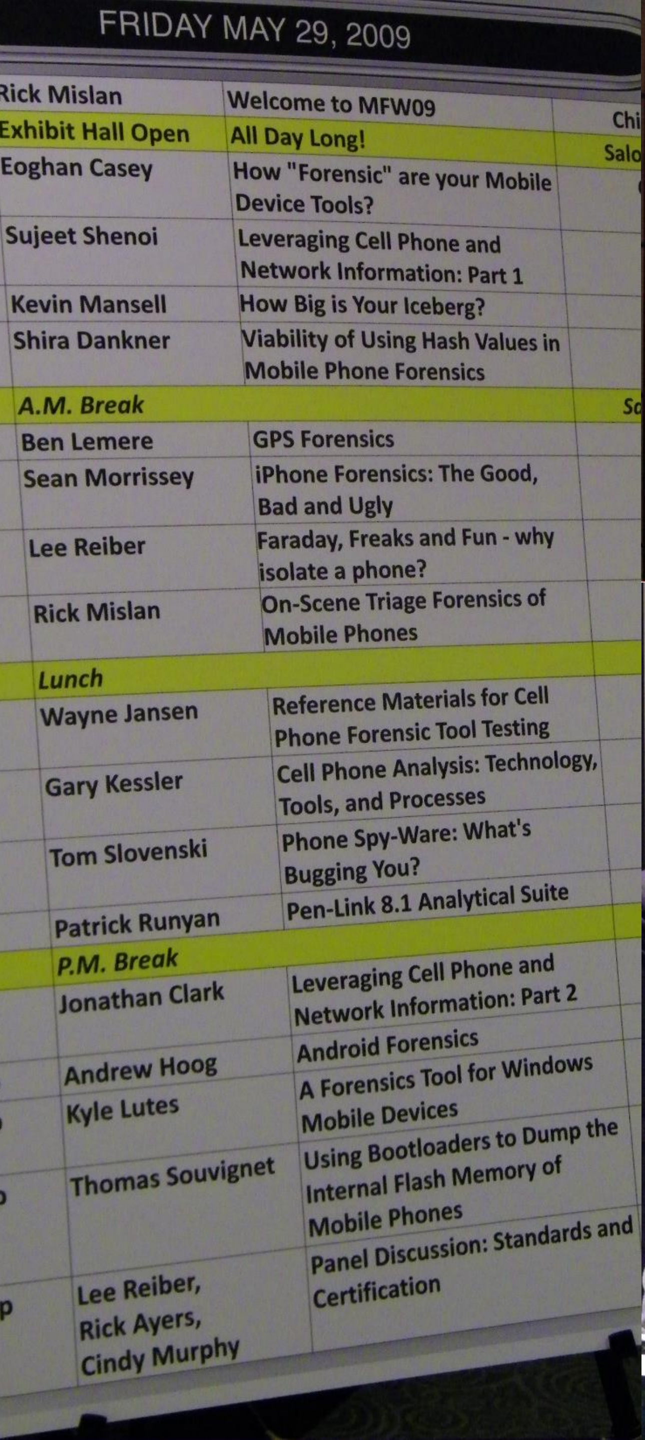
MOBILE FORENSICS WORLD 2008
CHICAGO
CHICAGO, IL, USA
MAY 8 - 10, 2008

MOBILE FORENSICS WORLD 2008
CHICAGO, ILLINOIS, USA - MAY 8-10, 2008

MOBILE FORENSICS WORLD 2009
MOBILE FORENSICS WORLD 2009
MOBILE FORENSICS WORLD 2009
MOBILE FORENSICS WORLD 2009
MOBILE FORENSICS WORLD 2009
MOBILE FORENSICS WORLD 2009
SK Telecom

MOBILE FORENSICS WORLD 09
CHICAGO, IL, USA
MAY 26-30, 2009

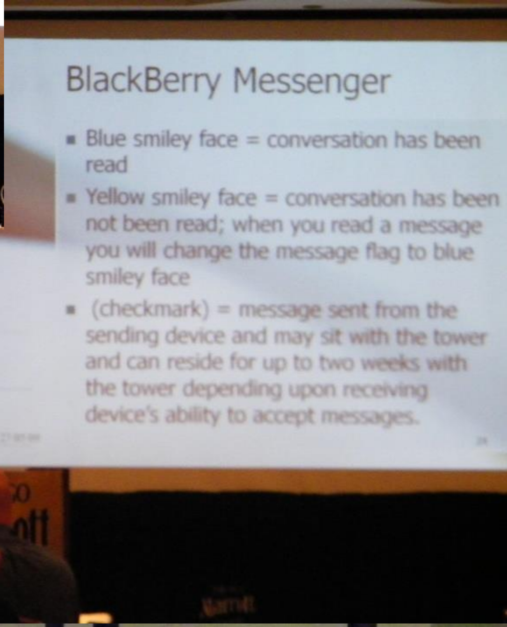
MOBILE FORENSICS WORLD
2010
THE YEAR
WE CONNECT
LLO DAVE



FRIDAY MAY 29, 2009

Rick Mislan	Welcome to MFW09	Chi
Exhibit Hall Open	All Day Long!	Salo
Eoghan Casey	How "Forensic" are your Mobile Device Tools?	
Sujeet Shenoi	Leveraging Cell Phone and Network Information: Part 1	
Kevin Mansell	How Big is Your Iceberg?	
Shira Dankner	Viability of Using Hash Values in Mobile Phone Forensics	
A.M. Break		Sa
Ben Lemere	GPS Forensics	
Sean Morrissey	iPhone Forensics: The Good, Bad and Ugly	
Lee Reiber	Faraday, Freaks and Fun - why isolate a phone?	
Rick Mislan	On-Scene Triage Forensics of Mobile Phones	
Lunch		
Wayne Jansen	Reference Materials for Cell Phone Forensic Tool Testing	
Gary Kessler	Cell Phone Analysis: Technology, Tools, and Processes	
Tom Slovenski	Phone Spy-Ware: What's Bugging You?	
Patrick Runyan	Pen-Link 8.1 Analytical Suite	
P.M. Break		
Jonathan Clark	Leveraging Cell Phone and Network Information: Part 2	
Andrew Hoog	Android Forensics	
Kyle Lutes	A Forensics Tool for Windows Mobile Devices	
Thomas Souvignet	Using Bootloaders to Dump the Internal Flash Memory of Mobile Phones	
Lee Reiber, Rick Ayers, Cindy Murphy	Panel Discussion: Standards and Certification	

Bridging the Gap Between Data and Evide



BlackBerry Messenger

- Blue smiley face = conversation has been read
- Yellow smiley face = conversation has been not been read; when you read a message you will change the message flag to blue smiley face
- (checkmark) = message sent from the sending device and may sit with the tower and can reside for up to two weeks with the tower depending upon receiving device's ability to accept messages.

Mobile Forensics: A Path Forward

May 28, 2009

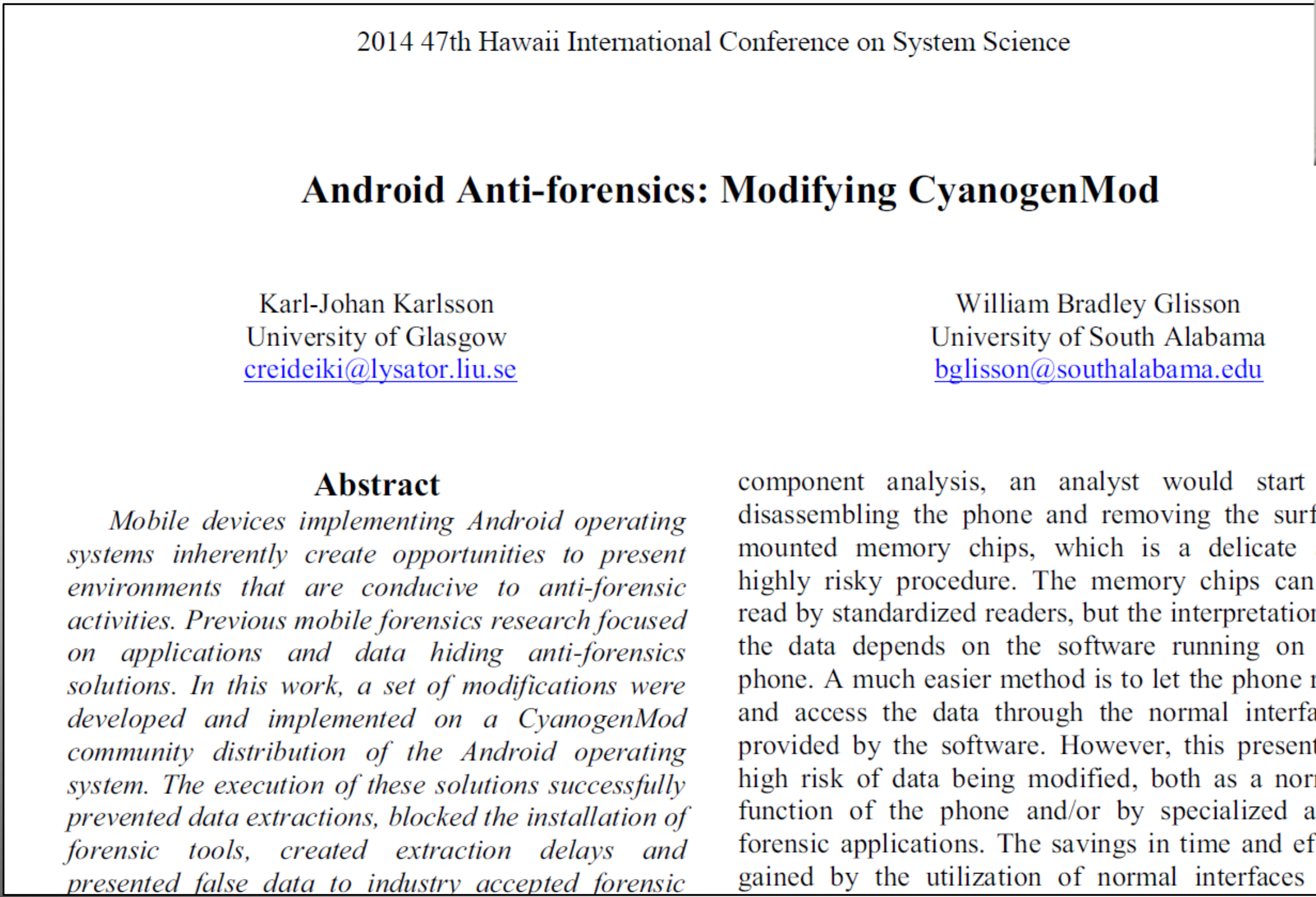
SSA Rick Voss
Federal Bureau of Investigation

Unclassified/FOUO

A Call to Arms

An Invitation for Research

National Institute of Standards and Technology
U.S. Department of Commerce



2014 47th Hawaii International Conference on System Science

Android Anti-forensics: Modifying CyanogenMod

Karl-Johan Karlsson
University of Glasgow
creideiki@lysator.liu.se

William Bradley Glisson
University of South Alabama
bglisson@southalabama.edu

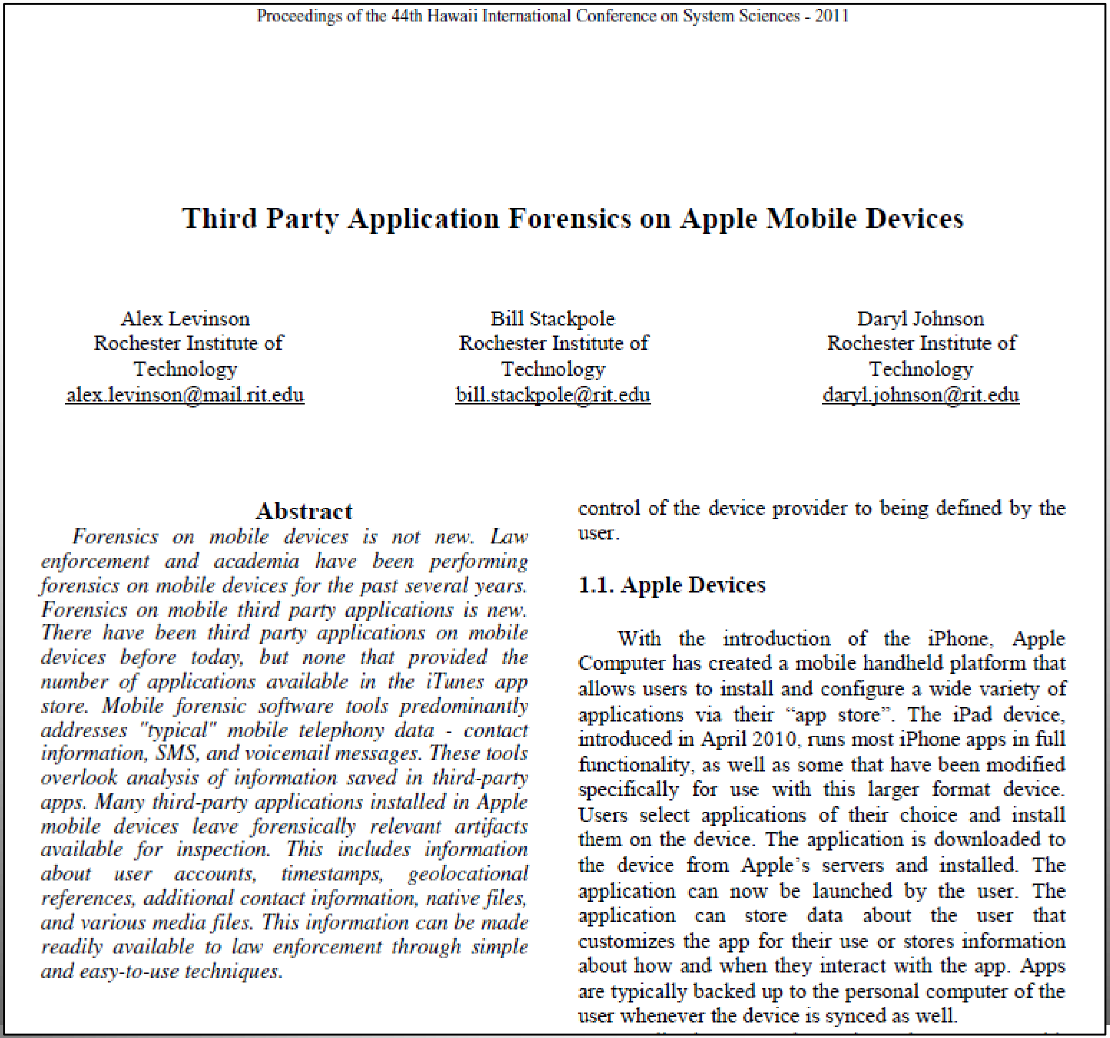
Abstract

Mobile devices implementing Android operating systems inherently create opportunities to present environments that are conducive to anti-forensic activities. Previous mobile forensics research focused on applications and data hiding anti-forensics solutions. In this work, a set of modifications were developed and implemented on a CyanogenMod community distribution of the Android operating system. The execution of these solutions successfully prevented data extractions, blocked the installation of forensic tools, created extraction delays and presented false data to industry accepted forensic

component analysis, an analyst would start by disassembling the phone and removing the surface mounted memory chips, which is a delicate and highly risky procedure. The memory chips can be read by standardized readers, but the interpretation of the data depends on the software running on the phone. A much easier method is to let the phone run, and access the data through the normal interfaces provided by the software. However, this presents a high risk of data being modified, both as a normal function of the phone and/or by specialized anti-forensic applications. The savings in time and effort gained by the utilization of normal interfaces are

Anti-Forensics

App Forensics



Proceedings of the 44th Hawaii International Conference on System Sciences - 2011

Third Party Application Forensics on Apple Mobile Devices

Alex Levinson
Rochester Institute of Technology
alex.levinson@mail.rit.edu

Bill Stackpole
Rochester Institute of Technology
bill.stackpole@rit.edu

Daryl Johnson
Rochester Institute of Technology
daryl.johnson@rit.edu

Abstract

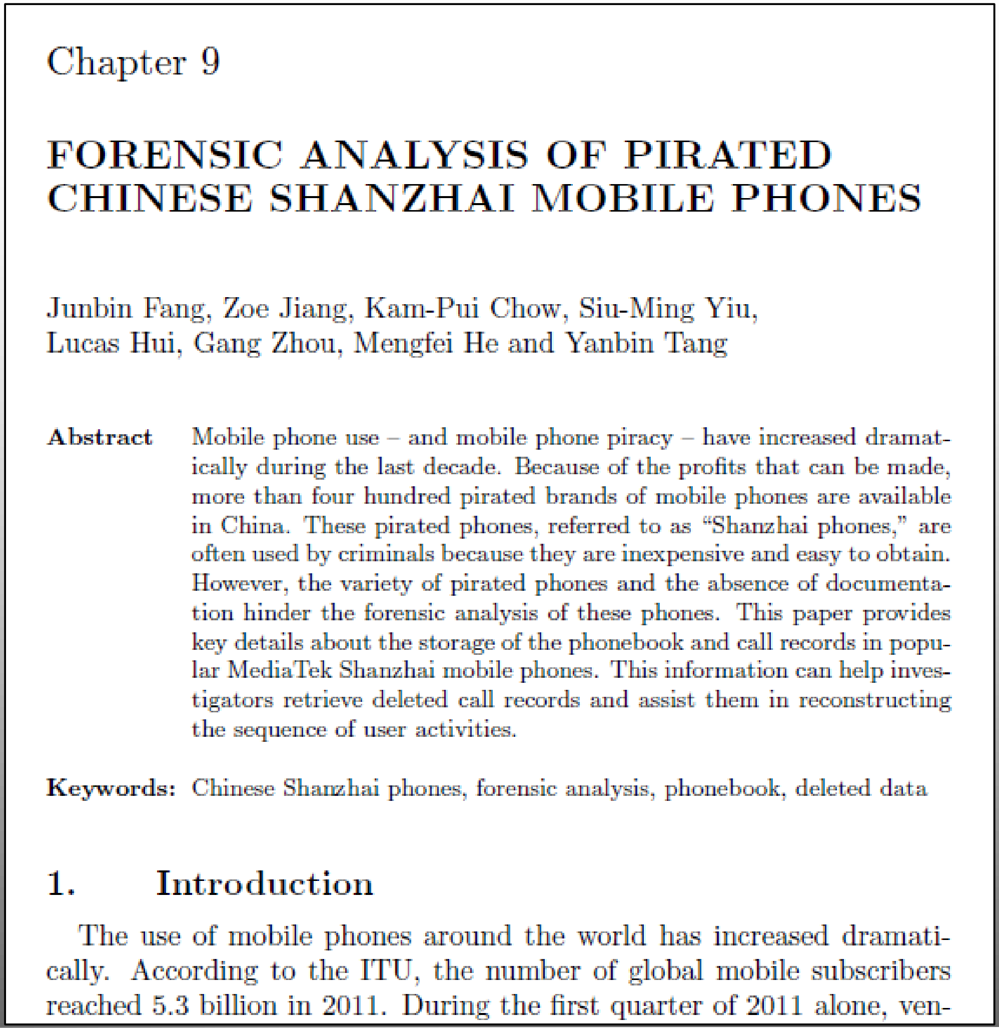
Forensics on mobile devices is not new. Law enforcement and academia have been performing forensics on mobile devices for the past several years. Forensics on mobile third party applications is new. There have been third party applications on mobile devices before today, but none that provided the number of applications available in the iTunes app store. Mobile forensic software tools predominantly addresses "typical" mobile telephony data - contact information, SMS, and voicemail messages. These tools overlook analysis of information saved in third-party apps. Many third-party applications installed in Apple mobile devices leave forensically relevant artifacts available for inspection. This includes information about user accounts, timestamps, geolocational references, additional contact information, native files, and various media files. This information can be made readily available to law enforcement through simple and easy-to-use techniques.

control of the device provider to being defined by the user.

1.1. Apple Devices

With the introduction of the iPhone, Apple Computer has created a mobile handheld platform that allows users to install and configure a wide variety of applications via their "app store". The iPad device, introduced in April 2010, runs most iPhone apps in full functionality, as well as some that have been modified specifically for use with this larger format device. Users select applications of their choice and install them on the device. The application is downloaded to the device from Apple's servers and installed. The application can now be launched by the user. The application can store data about the user that customizes the app for their use or stores information about how and when they interact with the app. Apps are typically backed up to the personal computer of the user whenever the device is synced as well.

Chinese Knockoffs



Chapter 9

FORENSIC ANALYSIS OF PIRATED CHINESE SHANZHAI MOBILE PHONES

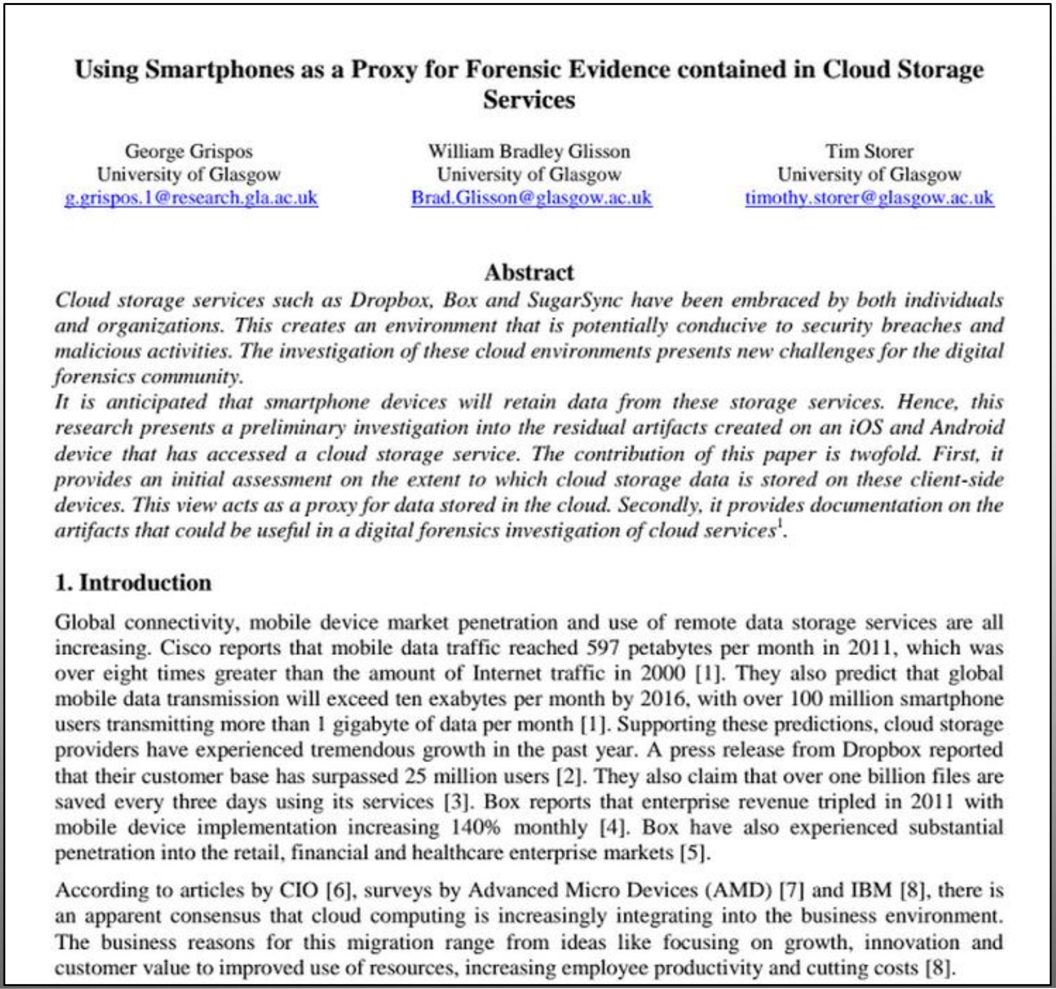
Junbin Fang, Zoe Jiang, Kam-Pui Chow, Siu-Ming Yiu,
Lucas Hui, Gang Zhou, Mengfei He and Yanbin Tang

Abstract Mobile phone use – and mobile phone piracy – have increased dramatically during the last decade. Because of the profits that can be made, more than four hundred pirated brands of mobile phones are available in China. These pirated phones, referred to as "Shanzhai phones," are often used by criminals because they are inexpensive and easy to obtain. However, the variety of pirated phones and the absence of documentation hinder the forensic analysis of these phones. This paper provides key details about the storage of the phonebook and call records in popular MediaTek Shanzhai mobile phones. This information can help investigators retrieve deleted call records and assist them in reconstructing the sequence of user activities.

Keywords: Chinese Shanzhai phones, forensic analysis, phonebook, deleted data

1. Introduction

The use of mobile phones around the world has increased dramatically. According to the ITU, the number of global mobile subscribers reached 5.3 billion in 2011. During the first quarter of 2011 alone, ven-



Using Smartphones as a Proxy for Forensic Evidence contained in Cloud Storage Services

George Grispos
University of Glasgow
g.grispos.1@research.gla.ac.uk

William Bradley Glisson
University of Glasgow
Brad.Glisson@glasgow.ac.uk

Tim Storer
University of Glasgow
timothy.storer@glasgow.ac.uk

Abstract

Cloud storage services such as Dropbox, Box and SugarSync have been embraced by both individuals and organizations. This creates an environment that is potentially conducive to security breaches and malicious activities. The investigation of these cloud environments presents new challenges for the digital forensics community.

It is anticipated that smartphone devices will retain data from these storage services. Hence, this research presents a preliminary investigation into the residual artifacts created on an iOS and Android device that has accessed a cloud storage service. The contribution of this paper is twofold. First, it provides an initial assessment on the extent to which cloud storage data is stored on these client-side devices. This view acts as a proxy for data stored in the cloud. Secondly, it provides documentation on the artifacts that could be useful in a digital forensics investigation of cloud services[1].

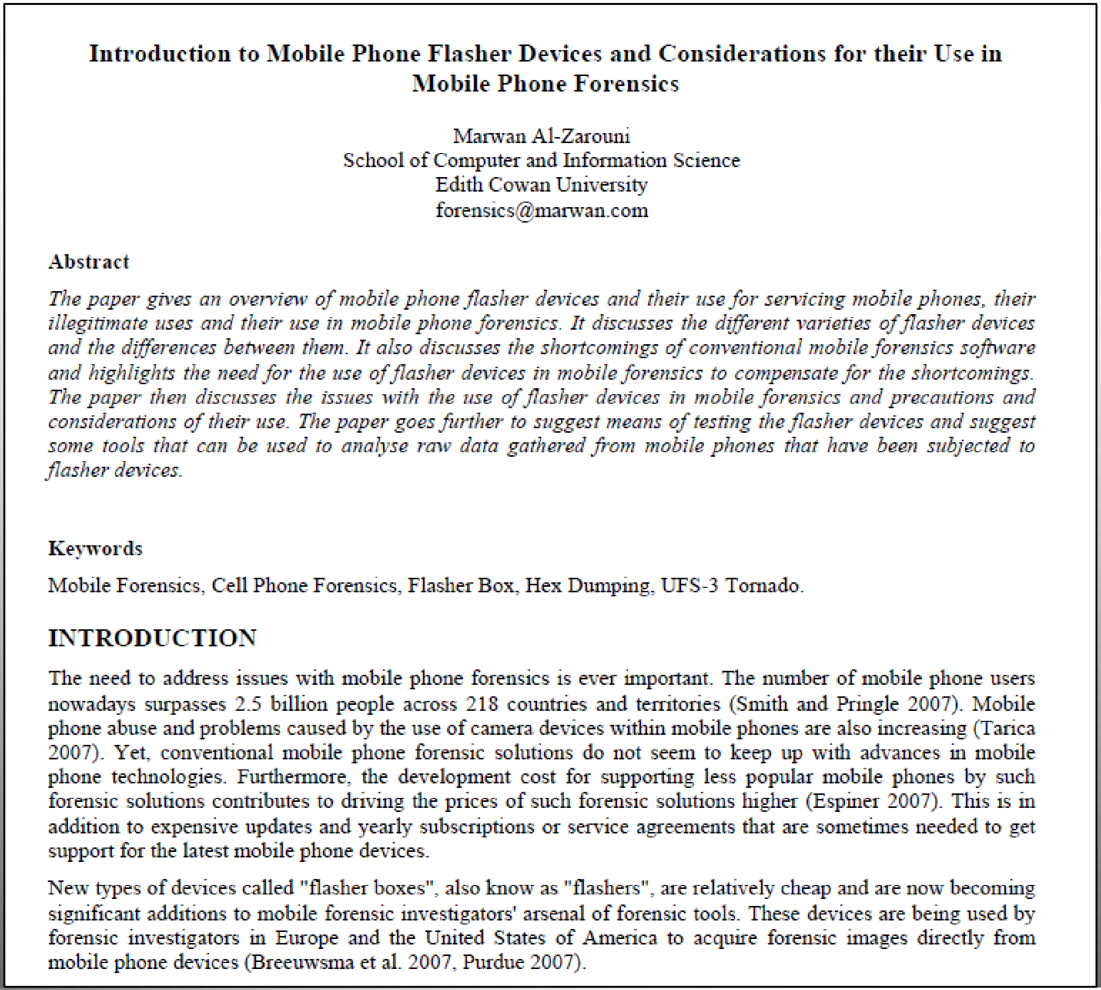
1. Introduction

Global connectivity, mobile device market penetration and use of remote data storage services are all increasing. Cisco reports that mobile data traffic reached 597 petabytes per month in 2011, which was over eight times greater than the amount of Internet traffic in 2000 [1]. They also predict that global mobile data transmission will exceed ten exabytes per month by 2016, with over 100 million smartphone users transmitting more than 1 gigabyte of data per month [1]. Supporting these predictions, cloud storage providers have experienced tremendous growth in the past year. A press release from Dropbox reported that their customer base has surpassed 25 million users [2]. They also claim that over one billion files are saved every three days using its services [3]. Box reports that enterprise revenue tripled in 2011 with mobile device implementation increasing 140% monthly [4]. Box have also experienced substantial penetration into the retail, financial and healthcare enterprise markets [5].

According to articles by CIO [6], surveys by Advanced Micro Devices (AMD) [7] and IBM [8], there is an apparent consensus that cloud computing is increasingly integrating into the business environment. The business reasons for this migration range from ideas like focusing on growth, innovation and customer value to improved use of resources, increasing employee productivity and cutting costs [8].

The Cloud

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



Introduction to Mobile Phone Flasher Devices and Considerations for their Use in Mobile Phone Forensics

Marwan Al-Zarouni
School of Computer and Information Science
Edith Cowan University
forensics@marwan.com

Abstract

The paper gives an overview of mobile phone flasher devices and their use for servicing mobile phones, their illegitimate uses and their use in mobile phone forensics. It discusses the different varieties of flasher devices and the differences between them. It also discusses the shortcomings of conventional mobile forensics software and highlights the need for the use of flasher devices in mobile forensics to compensate for the shortcomings. The paper then discusses the issues with the use of flasher devices in mobile forensics and precautions and considerations of their use. The paper goes further to suggest means of testing the flasher devices and suggest some tools that can be used to analyse raw data gathered from mobile phones that have been subjected to flasher devices.

Keywords

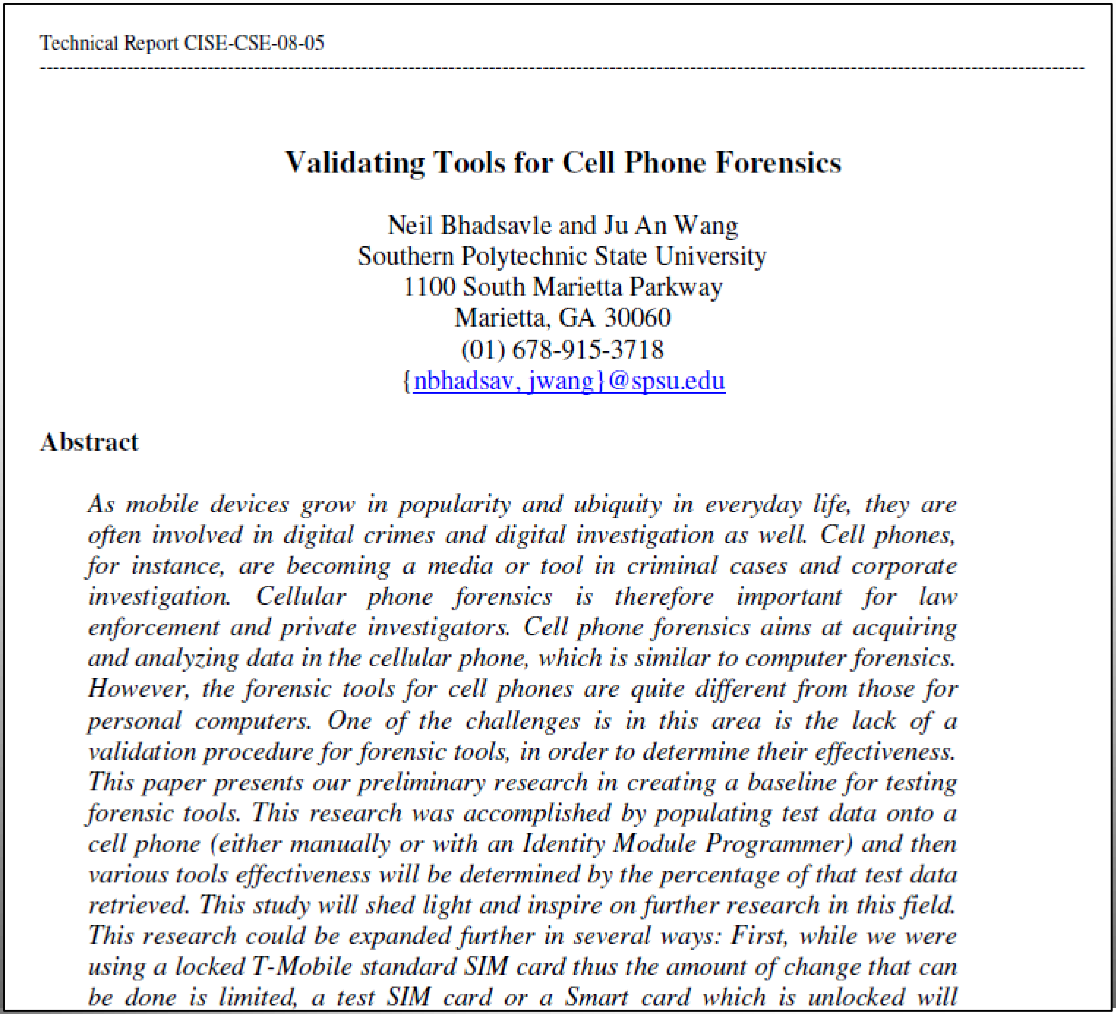
Mobile Forensics, Cell Phone Forensics, Flasher Box, Hex Dumping, UFS-3 Tornado.

INTRODUCTION

The need to address issues with mobile phone forensics is ever important. The number of mobile phone users nowadays surpasses 2.5 billion people across 218 countries and territories (Smith and Pringle 2007). Mobile phone abuse and problems caused by the use of camera devices within mobile phones are also increasing (Tarica 2007). Yet, conventional mobile phone forensic solutions do not seem to keep up with advances in mobile phone technologies. Furthermore, the development cost for supporting less popular mobile phones by such forensic solutions contributes to driving the prices of such forensic solutions higher (Espiner 2007). This is in addition to expensive updates and yearly subscriptions or service agreements that are sometimes needed to get support for the latest mobile phone devices.

New types of devices called "flasher boxes", also know as "flashers", are relatively cheap and are now becoming significant additions to mobile forensic investigators' arsenal of forensic tools. These devices are being used by forensic investigators in Europe and the United States of America to acquire forensic images directly from mobile phone devices (Breeuwsma et al. 2007, Purdue 2007).

Flasher Devices



Technical Report CISE-CSE-08-05

Validating Tools for Cell Phone Forensics

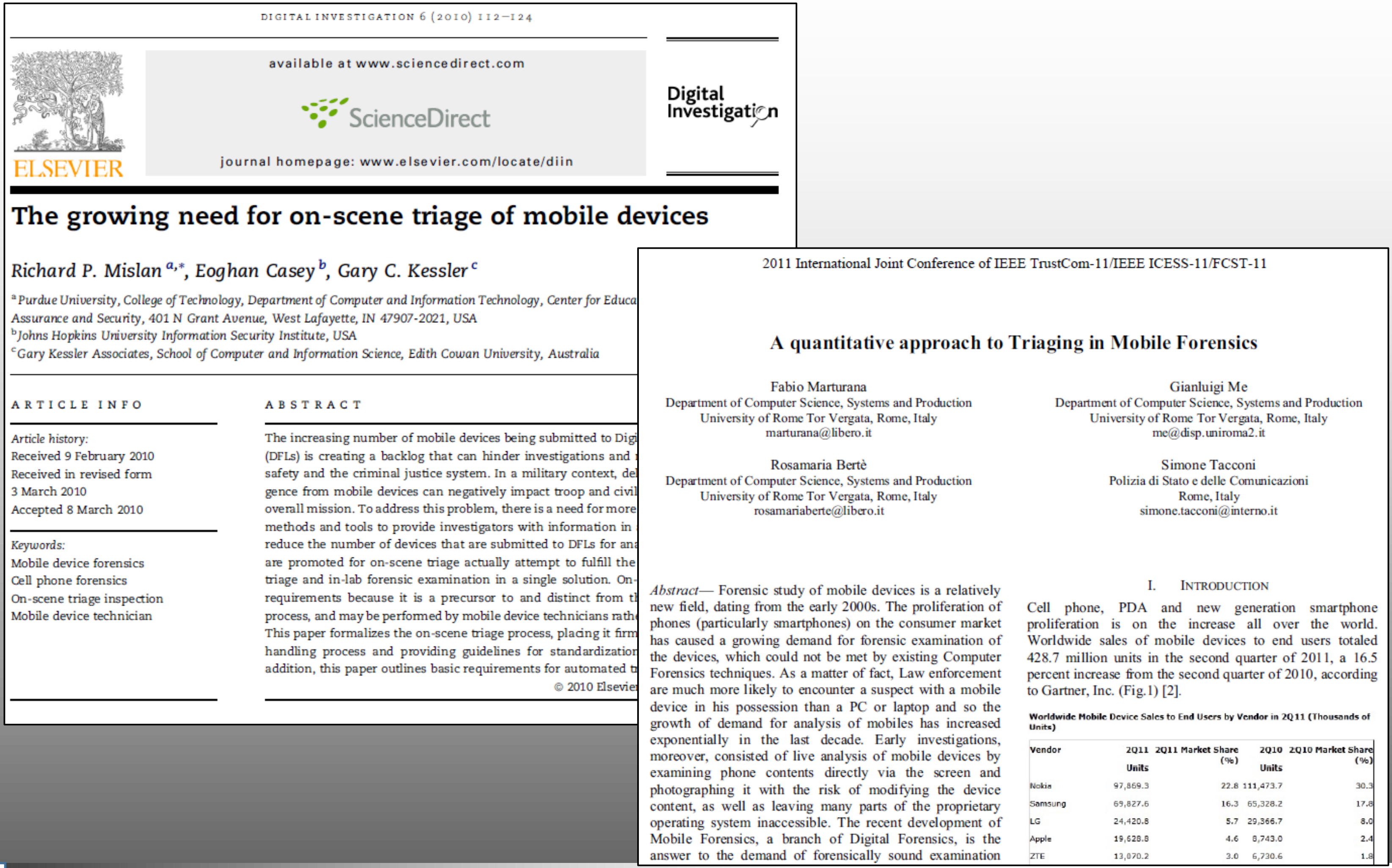
Neil Bhadsavle and Ju An Wang
Southern Polytechnic State University
1100 South Marietta Parkway
Marietta, GA 30060
(01) 678-915-3718
{nbhadsav, jwang}@spsu.edu

Abstract

As mobile devices grow in popularity and ubiquity in everyday life, they are often involved in digital crimes and digital investigation as well. Cell phones, for instance, are becoming a media or tool in criminal cases and corporate investigation. Cellular phone forensics is therefore important for law enforcement and private investigators. Cell phone forensics aims at acquiring and analyzing data in the cellular phone, which is similar to computer forensics. However, the forensic tools for cell phones are quite different from those for personal computers. One of the challenges is in this area is the lack of a validation procedure for forensic tools, in order to determine their effectiveness. This paper presents our preliminary research in creating a baseline for testing forensic tools. This research was accomplished by populating test data onto a cell phone (either manually or with an Identity Module Programmer) and then various tools effectiveness will be determined by the percentage of that test data retrieved. This study will shed light and inspire on further research in this field. This research could be expanded further in several ways: First, while we were using a locked T-Mobile standard SIM card thus the amount of change that can be done is limited, a test SIM card or a Smart card which is unlocked will

Tool Validation

National Institute of Standards and Technology
U.S. Department of Commerce



DIGITAL INVESTIGATION 6 (2010) 112–124

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

ELSEVIER

Digital Investigation

The growing need for on-scene triage of mobile devices

Richard P. Mislan [a],*, Eoghan Casey [b], Gary C. Kessler [c]

[a] Purdue University, College of Technology, Department of Computer and Information Technology, Center for Educa
Assurance and Security, 401 N Grant Avenue, West Lafayette, IN 47907-2021, USA
[b] Johns Hopkins University Information Security Institute, USA
[c] Gary Kessler Associates, School of Computer and Information Science, Edith Cowan University, Australia

ARTICLE INFO

Article history:
Received 9 February 2010
Received in revised form
3 March 2010
Accepted 8 March 2010

Keywords:
Mobile device forensics
Cell phone forensics
On-scene triage inspection
Mobile device technician

ABSTRACT

The increasing number of mobile devices being submitted to Digi
(DFLs) is creating a backlog that can hinder investigations and
safety and the criminal justice system. In a military context, de
gence from mobile devices can negatively impact troop and civil
overall mission. To address this problem, there is a need for more
methods and tools to provide investigators with information in
reduce the number of devices that are submitted to DFLs for an
are promoted for on-scene triage actually attempt to fulfill the
triage and in-lab forensic examination in a single solution. On-
requirements because it is a precursor to and distinct from th
process, and may be performed by mobile device technicians rath
This paper formalizes the on-scene triage process, placing it firm
handling process and providing guidelines for standardization
addition, this paper outlines basic requirements for automated t

2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11

A quantitative approach to Triaging in Mobile Forensics

Fabio Marturana
Department of Computer Science, Systems and Production
University of Rome Tor Vergata, Rome, Italy
marturana@libero.it

Gianluigi Me
Department of Computer Science, Systems and Production
University of Rome Tor Vergata, Rome, Italy
me@disp.uniroma2.it

Rosamaria Bertè
Department of Computer Science, Systems and Production
University of Rome Tor Vergata, Rome, Italy
rosamariaberte@libero.it

Simone Tacconi
Polizia di Stato e delle Comunicazioni
Rome, Italy
simone.tacconi@interno.it

Abstract— Forensic study of mobile devices is a relatively new field, dating from the early 2000s. The proliferation of phones (particularly smartphones) on the consumer market has caused a growing demand for forensic examination of the devices, which could not be met by existing Computer Forensics techniques. As a matter of fact, Law enforcement are much more likely to encounter a suspect with a mobile device in his possession than a PC or laptop and so the growth of demand for analysis of mobiles has increased exponentially in the last decade. Early investigations, moreover, consisted of live analysis of mobile devices by examining phone contents directly via the screen and photographing it with the risk of modifying the device content, as well as leaving many parts of the proprietary operating system inaccessible. The recent development of Mobile Forensics, a branch of Digital Forensics, is the answer to the demand of forensically sound examination

I. Introduction

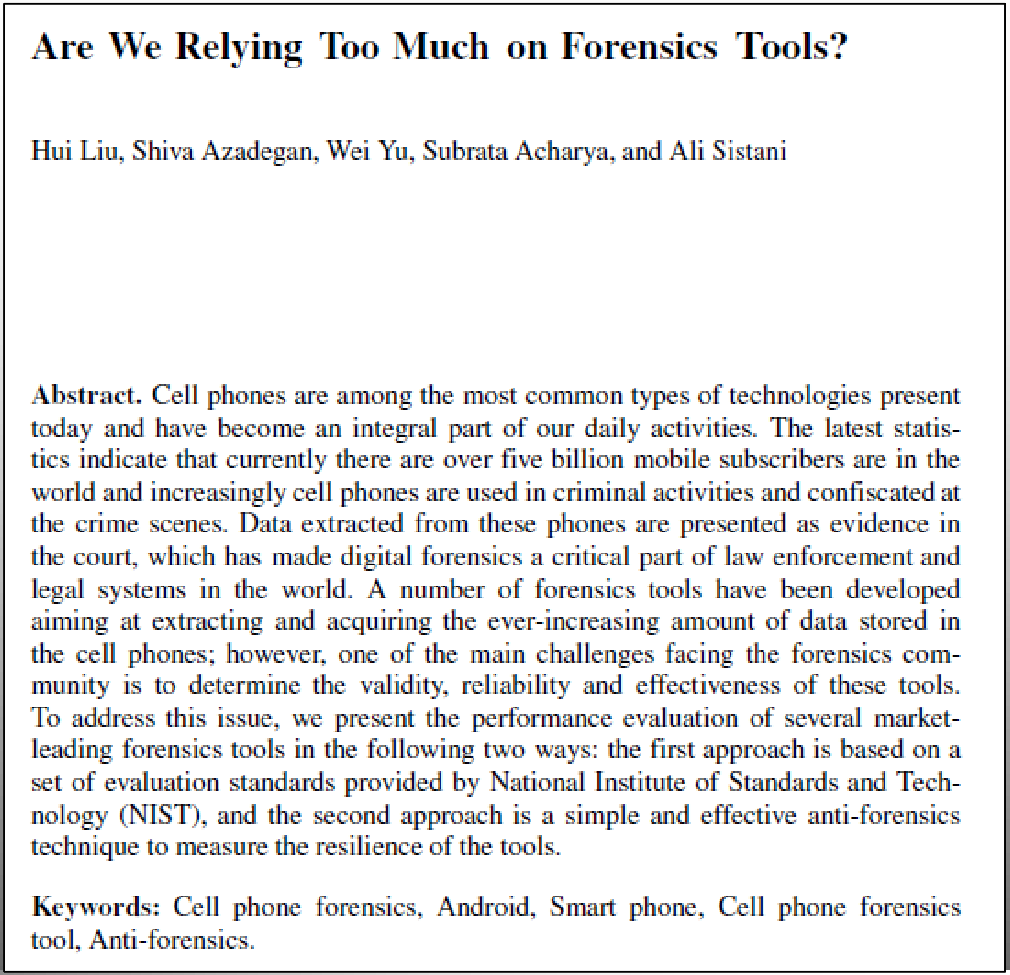
Cell phone, PDA and new generation smartphone proliferation is on the increase all over the world. Worldwide sales of mobile devices to end users totaled 428.7 million units in the second quarter of 2011, a 16.5 percent increase from the second quarter of 2010, according to Gartner, Inc. (Fig.1) [2].

Worldwide Mobile Device Sales to End Users by Vendor in 2Q11 (Thousands of Units)

Vendor	2Q11 Units	2Q11 Market Share (%)	2Q10 Units	2Q10 Market Share (%)
Nokia	97,869.3	22.8	111,473.7	30.3
Samsung	69,827.6	16.3	65,328.2	17.8
LG	24,420.8	5.7	29,366.7	8.0
Apple	19,628.8	4.6	8,743.0	2.4
ZTE	13,070.2	3.0	6,730.6	1.8

Triage

User Knowledge

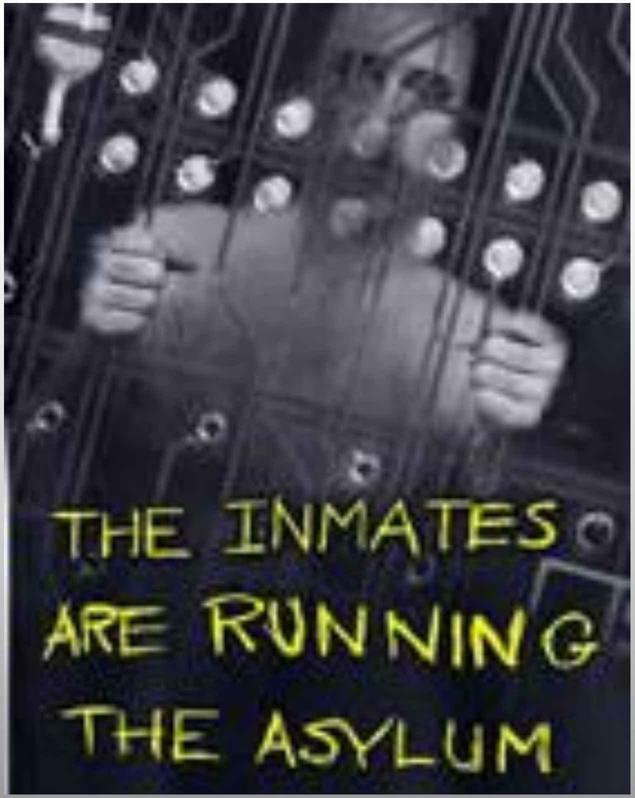


Are We Relying Too Much on Forensics Tools?

Hui Liu, Shiva Azadegan, Wei Yu, Subrata Acharya, and Ali Sistani

Abstract. Cell phones are among the most common types of technologies present today and have become an integral part of our daily activities. The latest statistics indicate that currently there are over five billion mobile subscribers are in the world and increasingly cell phones are used in criminal activities and confiscated at the crime scenes. Data extracted from these phones are presented as evidence in the court, which has made digital forensics a critical part of law enforcement and legal systems in the world. A number of forensics tools have been developed aiming at extracting and acquiring the ever-increasing amount of data stored in the cell phones; however, one of the main challenges facing the forensics community is to determine the validity, reliability and effectiveness of these tools. To address this issue, we present the performance evaluation of several market-leading forensics tools in the following two ways: the first approach is based on a set of evaluation standards provided by National Institute of Standards and Technology (NIST), and the second approach is a simple and effective anti-forensics technique to measure the resilience of the tools.

Keywords: Cell phone forensics, Android, Smart phone, Cell phone forensics tool, Anti-forensics.



The Vendor Tools

Ad Hoc Reactive Methodology

a. User Has an Issue
b. Emails Problem to Vendor
c. Fixes Issue in Next Revision

Validation and Verification

How do we know what we don't know!

New! Pre-sweetened Kool-Aid

It's sweetened without sugar to give you all the benefits and convenience of artificial sweetening. You just add water and ice —so it costs no more to make than regular Kool-Aid.

Now two kinds of Kool-Aid—new pre-sweetened *and* regular. Both make two quarts of pure, wholesome refreshment.

Drinking the Kool-Aid

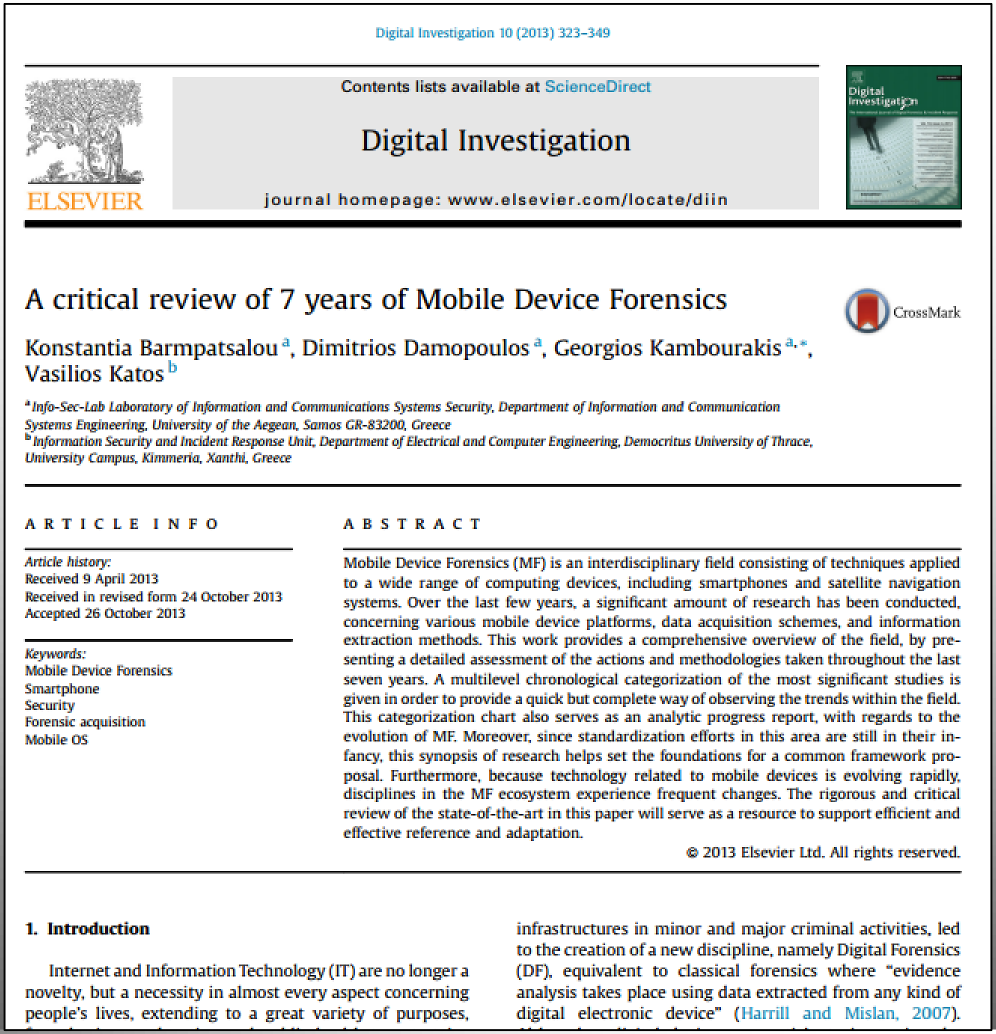
Research:

- Prove or disprove a hypothesis
- Learn new facts
- Advance the common body of knowledge

We have a need to know!

for Steve…

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



Digital Investigation 10 (2013) 323–349

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

A critical review of 7 years of Mobile Device Forensics

Konstantia Barmpatsalou[a], Dimitrios Damopoulos[a], Georgios Kambourakis[a,*], Vasilios Katos[b]

[a] Info-Sec-Lab Laboratory of Information and Communications Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, Samos GR-83200, Greece
[b] Information Security and Incident Response Unit, Department of Electrical and Computer Engineering, Democritus University of Thrace, University Campus, Kimmeria, Xanthi, Greece

ARTICLE INFO

Article history:
Received 9 April 2013
Received in revised form 24 October 2013
Accepted 26 October 2013

Keywords:
Mobile Device Forensics
Smartphone
Security
Forensic acquisition
Mobile OS

ABSTRACT

Mobile Device Forensics (MF) is an interdisciplinary field consisting of techniques applied to a wide range of computing devices, including smartphones and satellite navigation systems. Over the last few years, a significant amount of research has been conducted, concerning various mobile device platforms, data acquisition schemes, and information extraction methods. This work provides a comprehensive overview of the field, by presenting a detailed assessment of the actions and methodologies taken throughout the last seven years. A multilevel chronological categorization of the most significant studies is given in order to provide a quick but complete way of observing the trends within the field. This categorization chart also serves as an analytic progress report, with regards to the evolution of MF. Moreover, since standardization efforts in this area are still in their infancy, this synopsis of research helps set the foundations for a common framework proposal. Furthermore, because technology related to mobile devices is evolving rapidly, disciplines in the MF ecosystem experience frequent changes. The rigorous and critical review of the state-of-the-art in this paper will serve as a resource to support efficient and effective reference and adaptation.

1. Introduction

Internet and Information Technology (IT) are no longer a novelty, but a necessity in almost every aspect concerning people's lives, extending to a great variety of purposes,

infrastructures in minor and major criminal activities, led to the creation of a new discipline, namely Digital Forensics (DF), equivalent to classical forensics where “evidence analysis takes place using data extracted from any kind of digital electronic device” (Harrill and Mislan, 2007).

Historical Review

National Institute of Standards and Technology
U.S. Department of Commerce

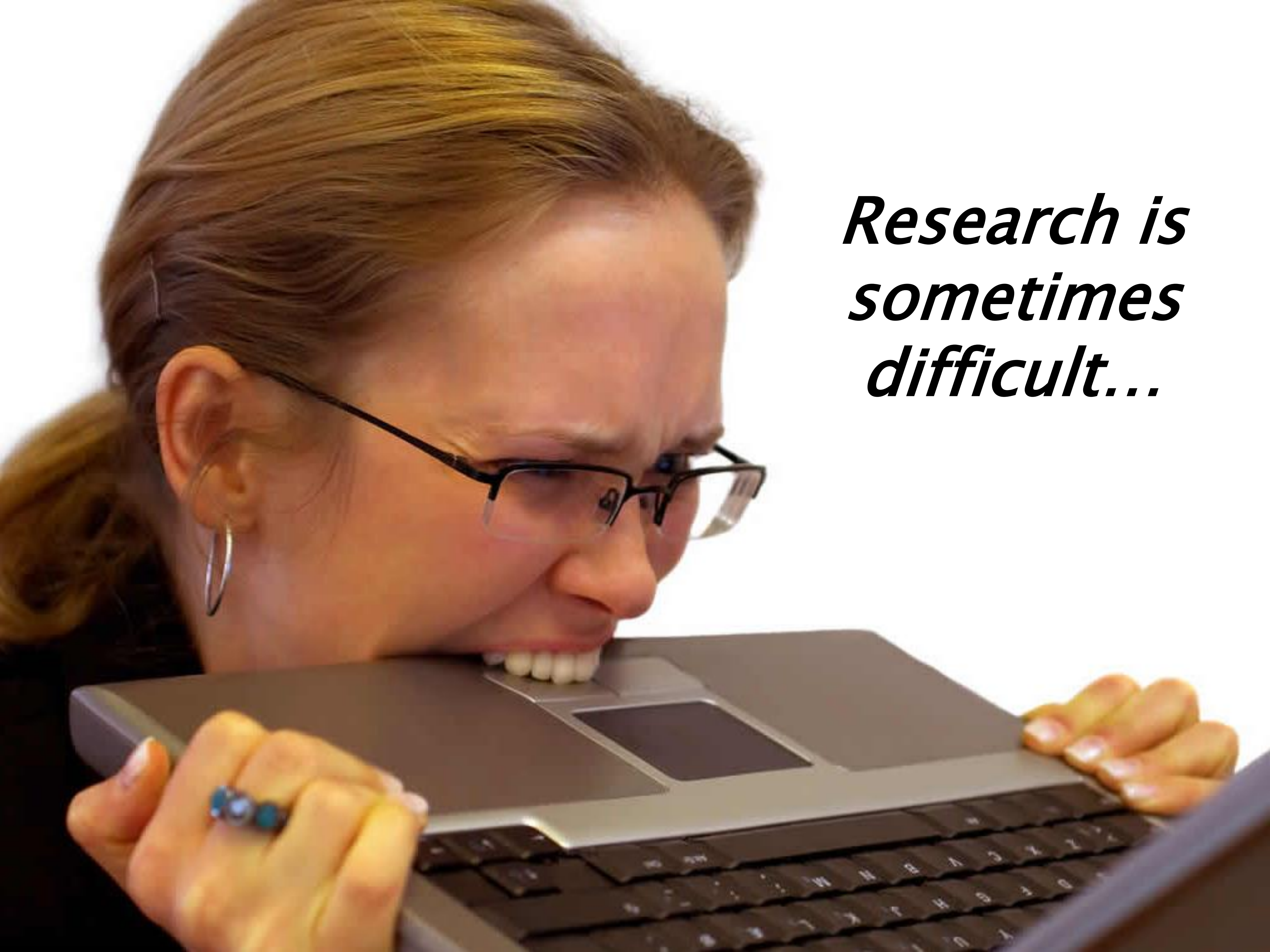
MOBILES!

WHAT HAVE WE LEARNED? WHERE ARE WE GOING?

DON'T WASTE YOUR MONEY

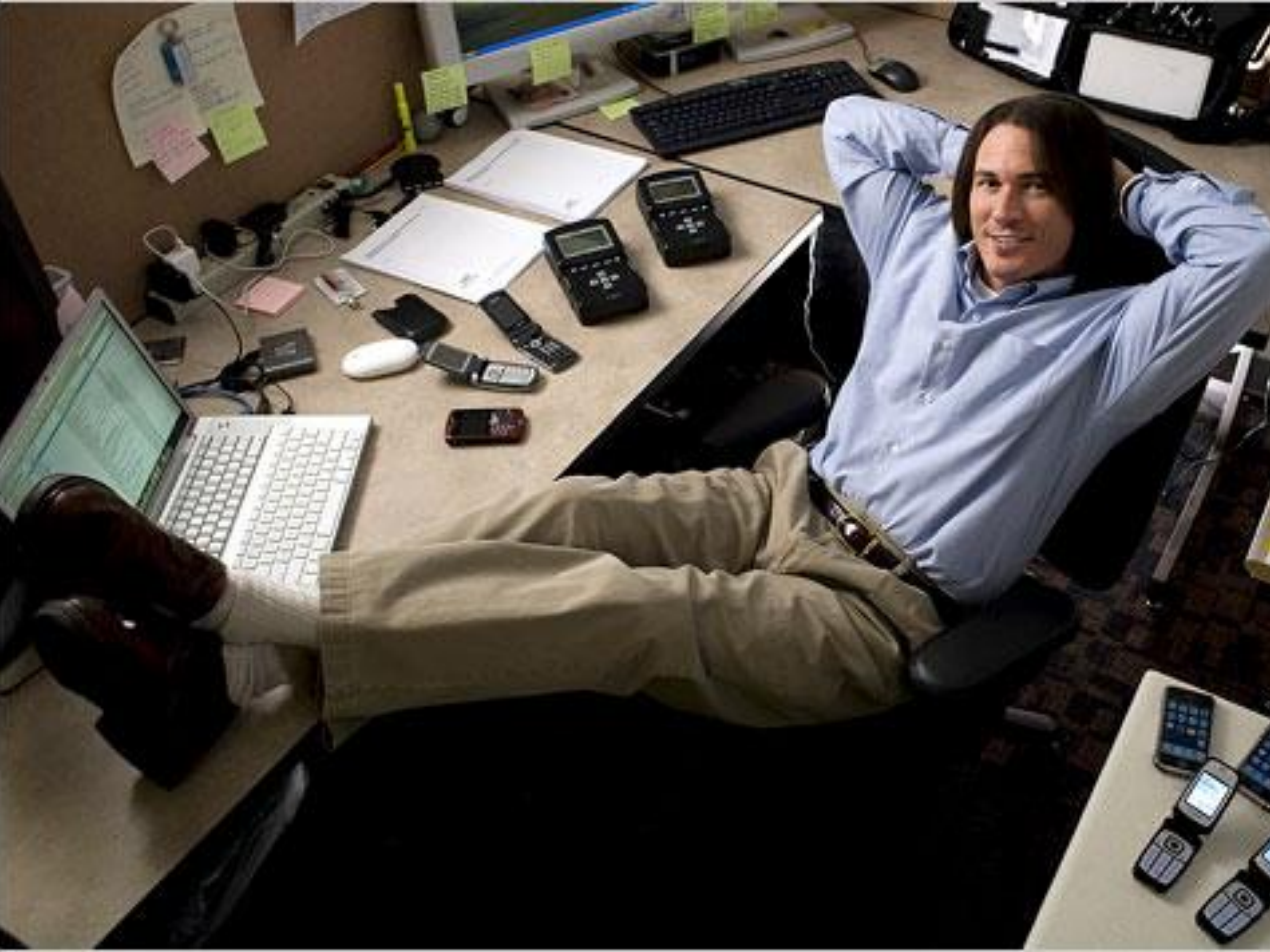
"PHABLETS" ARE COMING

COMBINE CELL PHONE AND TABLET

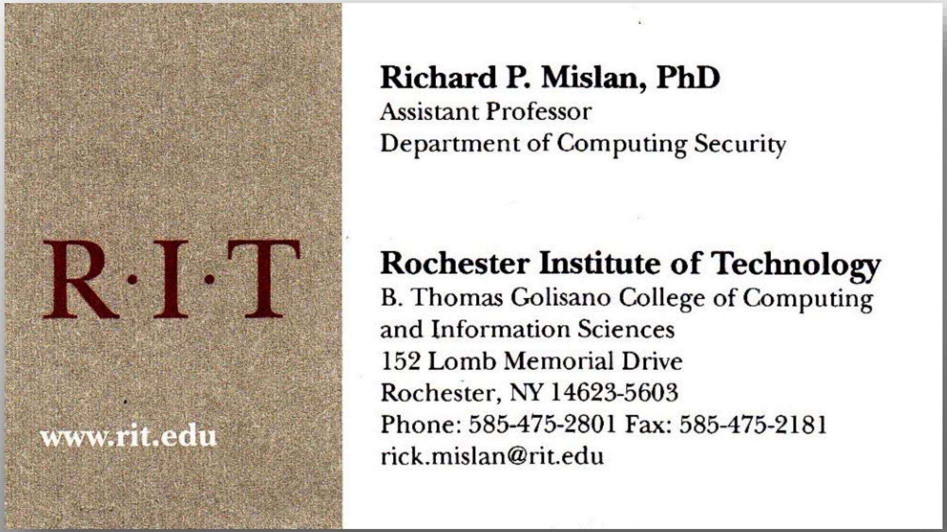


Research is sometimes difficult…

But,
research is
necessary!



Thank you!



R·I·T

www.rit.edu

Richard P. Mislan, PhD
Assistant Professor
Department of Computing Security

Rochester Institute of Technology
B. Thomas Golisano College of Computing
and Information Sciences
152 Lomb Memorial Drive
Rochester, NY 14623-5603
Phone: 585-475-2801 Fax: 585-475-2181
rick.mislan@rit.edu

www.mislan.com