Evaluation of Some Tools for Extracting e-Evidence from Mobile Devices

Appiah Kwame Kubi, Shahzad Saleem, Oliver Popov

Department of Computer and Systems Sciences
Stockholm University, Forum 100, Isafjordsgatan 39
SE- 16440 Kista, Sweden
{popov,okak,shahzads@dsv.su.se}

Abstract— **In a digital world, even illegal behaviour and/or crimes may be termed as digital. This world is increasing becoming mobile, where the basic computation and communication entities are Small Scale Digital Devices (SSDDs or S2D2s) such as ordinary mobile phones, personal digital assistants, smart phones and tablets. The need to recover data, which might refer to unlawful and unethical activities gave rise to the discipline of mobile forensics, which has become an integral part of digital forensics. Consequently, in the last few years there is an abundance of mobile forensics tools, both commercial and open-source ones, whose vendors and developers make various assertions about the capabilities and the performance of their tools. The complexity and the diversity of both mobile devices and mobile forensics tools, coupled with the volatile nature of the digital evidence and the legal requirements of admissibility makes it difficult for forensics investigators to select the right tool. Hence, we have evaluated UFED Physical Pro 1.1.3.8 and XRY 5.0 following "Smartphone Tool Specifications Standard" developed by NIST, in order to start developing a framework for evaluating and referencing the "goodness" of the mobile forensic tools. The experiments and the results of the research against the core smart phone tool specifications and their associated test findings are presented in such a way that it should make it easier for the prospective mobile forensic examiner select the most adequate tool for a specific case.**

***Keywords*— Digital Forensics, Mobile Device Forensics and tools, Reliability Assurance Level, and e-Evidence**

I. INTRODUCTION

Digital technology, usually epitomised by the computer and the Internet, has undeniably transformed almost every aspect of the contemporary societies including work, business, education, government, provision of various services such as health and disaster information and assistance, and entertainment. Criminal and in general illegal activities are no exception.

U.S. Census Bureau stated that the world population in December 01, 2010 was 6.884 billion (1) and ITU predicted 5 billion mobile subscriptions in 2010 (2), while the PEW Internet Report from 2009 forecasts that by 2020 most of the communication and computing would go through mobile devices. While mobility, which in many case makes time and location irrelevant for any kind of activities has brought immense benefits to the world, it has also created potent instruments for perpetuating and supporting unlawful and criminal deeds.

Although, mobile devices are relatively small in terms of their physical attributes, the communication and computing capabilities are constantly increasing by an order of magnitude within a period of a year or so. They are actually performing tasks similar to desktop and laptop computers such as transferring files, network connectivity, Internet access, running multimedia applications, emailing, and browsing. All these operations and functionalities indicate that significant number of traces of electronic evidence (e-Evidence) may be accumulated that are very likely to attract the interests of the forensic examiners.

While not every investigation is either subject to legal proceedings or intended to be used in the court of law, it is advisable to treat all the investigations with an anticipation that the evidence extracted and the subsequent forensic analysis of the data should be forensically sound or probative. In addition, the importance of using automated tools during forensics process is recommended in IOCE's guidelines to mitigate the risks of human errors (7). So, the tools, principles and methodology employed during mobile device forensics process must meet the requirements of legal admissibility stipulated by the Daubert Principle (8).

The huge number of mobile forensic tools appearing on the forensic arena almost daily are rarely subject to independent and scientific validation and verification. Most of the tests and evaluations are done by the vendors. Obviously, forensic examiners, bearing in mind the legal requirements for admissibility of the digital evidence, face the challenge of selecting the right tools which produce forensically sound evidence, hence probative and legally admissible.

Moreover, tools play a vital role in digital evidence processing and are used almost in all the phases of digital forensics process (9). So, it is important for a forensic examiner to know how reliable and accurate a tool is before being used. We have used the evaluation to gauge and verify the reliability and accuracy of two most prominent mobile forensic tools such as UFED Physical Pro 1.1.3.8 and XRY 5.0 based on the Smart Phone Tools Specifications by NIST (10).

This paper is organized as follows. The introductory section underlines the omnipresence of digital mobile devices in the digital society, the numerous benefits one side, and yet the

opportunities to use the same devices for illegal and unlawful activities on the other side. It posits also the need to have an independent and rigorous evaluation of these tools under the conditions of the Daubert principle. The second section describes the main characteristics of the discipline of digital forensics in general, enumerates the most important models of digital forensic investigation, and provides the key attributes of our model used later on the mobile devices. The section continues with the enumeration of the major digital forensic tools, and then introduces the salient requirements and features of mobile forensics, as well as the major components that must be considered and evaluated. The paper continues with the third section, which is the actual process of the evaluation of the tools. It starts with the methodology, and then gives the results of the process of the investigation against the mandatory functions as defined by the NIST requirements. Finally, the last section discussed the results of the evaluation and the comparative analysis, provides information on the additional ongoing research and outlines the next steps in this research endeavour on mobile forensics.

II. DIGITAL FORENSICS

Digital Forensics (DiFo) is a rapidly growing discipline in the field of Forensics Science, which began in the late 1980s and early 1990s [11, 12]. Since then, DiFo established a viable set of principles, methods, mechanisms and tools transcending through wide spectrum of domains that range from the law enforcement agencies to the military, business, industry organizations and institutions. Since it is a relatively new field many working groups and associations such as DFRWS, SWGDE, CART, NIJ and TWGDE have tried to formalize, standardize and mitigate inconsistencies in terminologies, definitions, processes, procedures and techniques that constitute the wide area of DiFo (11) (12).

A. Digital Forensics Process Models

Digital Forensics, which by its nature is exploratory, follows similar processes used by the law enforcement agencies during a crime scene investigation (13) (14). Since every investigation may have unique characteristics it is rather challenging to define a general digital forensic process model. Hence, one can find various models which are quite similar to certain extent such as the models proposed by US DOJ (15) and First DFRWS (16), the Abstract Digital Forensics Model (17), and Integrated Digital Investigation Model (18).

By working in a controlled laboratory environment, we have used our own model that is a derivation of the above enumerated models, and is based mostly on the different phases or stages as described below:

1. *Collection:* This stage deals with the collection of various potential sources of digital evidence e.g. mobile device both working and auxiliary storage, SIM cards etc.
2. *Identification:* The focus us on the recognition by labelling the potential sources of digital evidence.
3. *Acquisition:* Translates to the extraction of e-Evidence from various sources that have been captured and seized.
4. *Preservation:* Here the emphasises on using the adequate measures that ensure the integrity and the authenticity of digital evidence.
5. *Examination and Analysis:* It comprises of the activities such as searching, filtering, uncovering and examining/evaluation for relevance and probative value of the extracted e-Evidences.
6. *Reporting:* It is concerned with the presentation (in various forms such as written and oral) of the detailed summary and conclusions regarding the findings.

B. Digital Forensics Tools

Digital forensics (DiFo) experts use digital forensics tools to carry out their tasks effectively and efficiently, and complete their process of investigation in as much as possible unambiguous and transparent way. First generation DiFo Tools dates back to 1980s e.g. "dd" (19) (20). They were usually DOS based CLI driven tools targeting mainly data recovery on UNIX systems. The second generation tools evolved in 1990s and were already designed for forensics purposes with the appropriate graphical user interfaces (GUIs) for both UNIX and Windows systems such as NTI SafeBack, DIBS and Encase (20) (19). Nowdays, we work with the Third Generation DiFo tools capable of investigating live machines even remotely when required e.g. Encase Enterprise, Carnivore, NetIntercept, NFT Security, NetWitness and SilentRunner (20) (19).

With a rapid proliferation of mobile devices into our society which converges to omnipresence, the possibility to use these devices in adverse ways for carrying out nefarious activities mushroomed. This created an urgency to develop yet another category of DiFo tools termed as Mobile Device Forensics Tools such as Device Seizure, CellDEK, MobilEdit, PhonseBase2, BitPim, CelleBrite UFED System, XRY, FTK Mobile Phone Examiner, and Mobile Internal Acquisition Tool (21). The influx of commercial or proprietary tools has been accompanied with a myriad of open source tools as well, which makes it rather difficult for a DiFo investigator to decide what tool or tools are the most suitable ones for a given case. Knowing that each forensic investigation might have dare consequences on human life and property, posited the need for research into evaluation, comparative analysis and eventually grading the tools with respect to their performance in any kind of digital forensic investigations.

C. Mobile Device Forensics

While the benefits of mobility in the cyber space and in the contemporary societies are almost infinite, so are the opportunities for their abuse and sinister activities. Obvious examples include, but are not limited to, trafficking humans and illegal substances, unlawful financial transactions, invasion of privacy, taking images without permission, theft of intellectual property and identity, and data breaches of various sorts (3) (4) (5).

The domain of Mobile Forensics (MoFo), inter alia addresses the following phenomena:

1) *Mobile Devices:* Technological evolution has blurred the differences between a cell phone, a PDA and a smart phone.
    a. *Cell Phone:* A device with radio capabilities primarily used for voice communication, SMS and with few task management activities. Since, cell phones are continually incorporating different features of PDAs they are rightly classified into basic, advanced and high-end phones **Invalid source specified.**.
    b. *Personal Digital Assistant (PDA):* Traditionally PDAs were PIM devices with wide touch screens and networking capabilities (both local or the Internet). Today, PDAs have radio capabilities and run on different flavours of Mobile Operating Systems (for instance a PDA with MS Windows Mobile OS works almost a small minicomputer or a notebook). They may provide wireless connectivity, digital camera, keyboard and mobile versions of document management software.
    c. *Smartphone:* According to NIST Smartphone Tools Specifications it is a device with all the features of a mobile phone along with personal computer like functionality e.g. support of PIM applications, enhanced and rich internet features, accelerated processing, large storage capacity based on a mobile version of a laptop or even a desktop operating system. However, the literature research, as well as private communications with a brand name mobile phone manufacturing company and three mobile forensics tool vendors revealed that there is no industry standard definition of a "Smartphone".
2) *Sources of Evidence:* Potential sources of evidence associated with mobile devices are *Handset Memory*, *SIM Memory,* and *Memory Card*. This research is not concerned with investigation of memory cards since traditional forensics tools can handle them as well.
    a. Handset Memory: Following data objects can be extracted from it.
        i. PIM Entries
            1. Contacts entries
            2. Calendar entries
            3. Notes/Memo entries
            4. Task entries
        ii. Messaging Entries
            1. SMS
            2. EMS
            3. MMS
            4. Voice Messages
        iii. Call Logs
            1. Audio Calls
            2. Video Calls
        iv. Email Entries
        v. Internet History
            1. URLs Visited
            2. Bookmarks
        vi. Standalone Files
            1. Audio Files
            2. Video Files
            3. Graphic/Picture Files
        vii. Application Related Files
            1. Word Files
            2. Excel Files
            3. PowerPoint Files
            4. PDF Files
            5. OneNote Files
        viii. GPS Entries
        ix. Device Information e.g. IMEI, ESN, MEID and System Firmware etc.
    b. *SIM Memory:* Data objects that can be retrieved from SIM Memory include:
        i. Service Related Information
            1. ICCID
            2. IMSI
            3. MSISDN
            4. SPN
            5. SDN
        ii. Phonebook Information
            1. ADN
            2. FDN, when allowed by network provider.
        iii. Call Information: LND
        iv. Messaging Information
            1. SMS
            2. EMS
        v. Location Information
            1. LOCI
            2. LOCI GPRS

III. Tool Evaluation

In this section we will elaborate how the tools were populated with data objects and evaluated. For evaluation, we have used "Validation approach" since the tools were of propitiatory nature and there was no access to their documentation and source code.

D. Evaluation Methodology

We will evaluate both the tools in the light of NIST Smartphone Tool Specification which consists of a number of specifications with their associated Test Assertions and Conformance Indicators. These specifications with their associated assertions are further classified into "Core" and "Optional" ones. In this paper; however, we will limit ourselves to test and evaluate compulsory smart phone tool specifications along with their corresponding test assertions. We will present the result of our evaluation graphically to help in deciding the right tool for the right job. The evaluation

results will also help the respective vendors to improve their products.

E. Tools Overview

Before proceeding to present our results, it is necessary to provide a brief overview of the tools and devices used during the evaluation process.

1. *UFED Physical Pro:* Universal Forensic Extraction Device Physical Professional (UFED Physical Pro) is a mobile forensics tool developed by Cellebrite. Cellebrite is a fully owned subsidiary of Sun Corporations, established in 1999 and based in Israel. The vendor supports over 2000 handset models for logical extraction and over 500 models for physical extraction. It is hardware based rugged device that comes with software for both logical and physical examination.
2. *XRY:* Developed by Micro Systemation, version 5.0 works for both logical and physical extraction. Micro Systemation was founded in 1984 and is based in Sweden. XRY supports somewhere between 1500 to 1600 handset models for logical extraction and between 400 to 500 handset models for physical extraction. Until the XRY 5.0 upgrade, it was software only which needs to be installed on a computer. The field versions come with a PC tablet and pre-installed software.

F. Population of Data Objects

Following the methodology introduced by **Invalid source specified.**, three different methods exist for data population and we have used all three in our research.

1) *Manual:* Populating data objects by handset user interface.
2) *Semi Manual:* Copying or transferring data objects from same or similar mobile device to other.
3) *Automatic:* Using an application or scripting tool to populate data objects into a mobile device.

To avoid any wrong interpretation and analysis of extracted digital evidence, initial states of handsets were acquired and kept safe as "control states" within our reference space. Current date and time was also set before populating the devices.

1) Sony Ericsson Xperia X1

a. PIM Entries: These entries were created collaboratively using Xperia X1, Nokia 5800 and MS Office Outlook 2007. Contacts consist of special characters, blank entries, associated email addresses and pictures etc. A total of 631 entries were populated. Out of these, 15 were manually deleted.

b. Message Entries: Xperia X1 stores message entries in the internal memory. We used three types of message entries i.e. SMS entries composed of ASCII and Non-ASCII text messages, EMS entries made up of emoticons and MMS comprising audio, graphics and video messages. In total 339 such entries were populated, while 21 of them were manually deleted afterwards.

c. Call Log: Removal of the SIM does not affect call logs in Xperia X1. The population in this case was made out of 302 entries. Fourteen of them were manually deleted.

d. Emails: X1 was synchronized with an existing email account using WLAN. Some were also populated manually by creating new emails and replying to incoming emails. In total 444 were populated and 399 were manually deleted out of 444.

e. Internet History: In this case, 500 entries were populated by browsing the Internet using WLAN. Only 10 out of 500 were manually deleted.

f. Standalone Files: There were 1629 entries in the population, and 386 out of these 1629 were manually deleted.

g. Application Files: A total of 438 office and PDF files were populated and 5 out of them were manually deleted.

h. GPS Entries: Pictures with associated GPS metadata were populated.

2) Nokia 5800 Express Music

a. PIM Entries: These entries were created collaboratively using Xperia X1, Nokia 5800 and MS Office Outlook 2007. Contacts are made of special characters, blank entries, associated email addresses and pictures etc. A total of 555 entries were populated. Out of these, 10 were manually deleted.

b. Message Entries: Nokia 5800 stores message entries in its internal memory. We used three types of message entries such as SMS entries composed of ASCII and Non-ASCII text messages, EMS entries made up emoticons and MMS comprising audio, graphics and video messages. Exactly 317 such entries were populated, while 10 of them were manually deleted afterwards.

c. Call Log: Call logs are lost when SIM card is removed. Total 253 entries were populated, 5 of them were manually deleted. Some were deleted while changing the SIM card and for all practical purposes were considered valid entries.

d. Emails: Nokia 5800 was synchronized with an existing email account using WLAN. Some were also populated manually by creating new emails and replying to incoming emails. In total 389 were populated. None were deleted since deletion only marks the entry for deletion and keeps the headers until synchronized with the appropriate email server.

e. Internet History: Exactly 500 entries were populated by browsing internet using WLAN. In this case, 20 out of 500 were manually deleted.

f. Standalone Files: In total, 1709 entries were populated and 155 were manually deleted.

g. Application Files: The number of office and PDF files that were populated was 437, and 5 out of them were manually deleted.

h. GPS Entries: Pictures with associated GPS metadata were populated.

3) SIM Card:

a. PIM: Entries were populated manually and also copied from internal memory to the SIM card for both the smart phones. Total 246 entries were populated.

b. Message: A total of 30 entries were populated and then 10 were deleted manually.

c. Call Log: In this case, 11 entries in total were populated.

G. Evaluation Process

The evaluation process was carried out by following forensic model introduced in Section II.

1) *Collection:* Mobile devices with potential containers of digital evidences were the property of the Cyber Scene Investigation lab at DSV. The devices were interacted in a controlled environment, which somewhat relaxed the conditions for data collection.

2) *Identification:*

TABLE III
IDENTIFICATION OF XPERIA X1

Handset	Sony Ericsson Xperia X1
Manufacturer	Sony Ericsson
Model No	Xli
Platform	Microsoft Windows Mobile 6.1
IMEI	357263020058437
CPU	QUALCOMM (R) 7200A
Speed	528 MHz
Protocol Version	52.65.25.34U

TABLE IIv
IDENTIFICATION OF NOKIA 5800

Handset	Nokia 5800 XpressMusic
Manufacturer	Nokia
Model No	Nokia 5800 XpressMusic
Platform	Symbian OS v9.4, Series 60 rel. 5
IMEI	354182020014294
CPU	ARM 11
Software Version	20.0.012
Speed	434 MHz

TABLE V
IDENTIFICATION OF SIM

SIM Provider	Lycatel
Serial Number	8946120809221669018
MSISDN	+46761589655
Phonebook Size	250
Maximum Length of Name	30
Maximum Length of Number	Varies with handset used.
SMS Message Storage Capacity	30
SIM Provider	Lycatel

3) Preservation of Digital Evidence: We wanted to use cloned SIM Cards in the mobile devices to ensure the integrity of e-Evidence in the internal memory of the mobile devices. Subsequently, we cloned the SIM cards by using the tools before populating any data objects. Then we analysed the contents of evidence extracted after inserting the cloned SIM with our control data. Results showed no variation in the two evaluated tools.

4) Extraction of e-Evidence: While Xperia X1 is supported for both logical and physical extraction, Nokia 5800 was limited to logical extraction.

5) Examination: Both tools facilitate examination process by detailed reports and searching tools.

6) Analysis: Data elements extracted by the tools were examined and analysed with the help of control data and already known data from the population stage. Reliability assurance levels were computed by following the evaluation process introduced above.

7) Reporting: This is addressed in the section were we discuss the findings and the results.

IV. RESULTS AND DISCUSSION

Each assertion was tested and if the actual and the expected result were identical then it is a pass with respect to a specific criteria, otherwise they were qualified as a fail.

The complete results were charted, where

- Pass is represented by 2
- Pass with Comments is represented by 1
- Assertion not tested is represented by 0
- Fail is represented by -1
- Result 1 is for Nokia 5800 and SIM with XRY 5.0
- Result 2 is for Sony Ericsson Xperia X1 and SIM with XRY 5.0
- Result 3 is for Nokia 5800 and SIM with UFED 1.1.3.8
- Result 4 is for Sony Ericsson Xperia X1 and SIM with UFED 1.1.3.8

Assertions are represented on x-axis and results on y-axis.

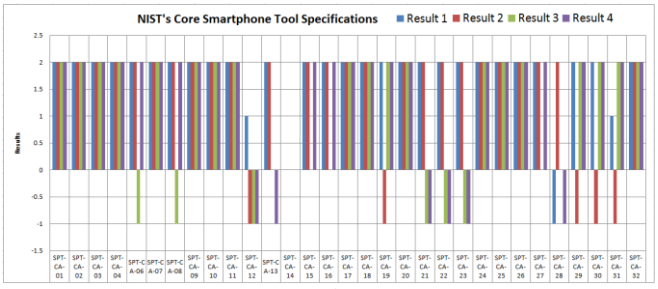

Fig. 1 Core Smartphone Tool Specifications (Both Tools Combined)

V. Conclusion

The research was focused on the evaluation of XRY 5.0 and UFED 1.1.3.8 mobile forensic tools based on NIST Smartphone Tool Specification and corresponding Test Cases using Daubert Principle as a reference point towards the admissibility of Digital Evidence. We have also compared our results of evaluation by using graphical representation which showed that in most of the cases XRY 5.0 outperformed UFED 1.1.3.8. This chart can be used by an examiner for selecting the right tool for a specific case by considering the relevant results. The ongoing work includes the representation of all the optional specifications and their associated test assertions. The combined results of evaluating both compulsory and optional specifications should provide a complete picture of the capabilities and the performance of two very important mobile forensics tools on the market and used as a frame of reference for any other similar tools, especially in the area of open source ones.

This paper presents the findings with respect to the reliability of the tools only. The next paper, which is also part of the ongoing research in the CSI lab, should report on the statistical validity and the associated inferential statistics. Moreover, the extension of the research that deals with other tools and larger pool of mobile devices (smart phones including tablets) is under consideration as well.

VI References

1. **International Programs Center, U.S. Census Bureau.** International Programs. *U.S. Cnesus Bureau.* [Online] [Cited: 1 March 2011.] http://www.census.gov/ipc/www/popclockworld.html.

2. **International Telecommunication Union.** Newsroom, Press Release. *International Telecommunication Union.* [Online] ITU. [Cited: 1 March 2011.] http://www.itu.int/net/pressoffice/press_releases/2010/06.aspx.

3. **Ahonen, Tomi T.** *Mobile as 7th of the Mass Media Cellphone, Cameraphone, iPhone, Smartphone.* s.l. : FUTURETEXT, 2008. ISBN-13: 978-0955606953.

4. **McCullagh, Declan and Broache, Anne.** FBI taps cell phone mic as eavesdropping tool. *cnet news.* [Online] cnet, 1 December 2006. [Cited: 18 September 2010.] http://news.cnet.com/2100-1029-6140191.html.

5. *Flexispy.* [Online] 2006. [Cited: 18 September 2010.] http://www.flexispy.com/index.html.

6. *The SMS Murder Mystery: the dark side of technology.* **Burnett, Robert and Segerstad, Ylva Hård af.** s.l. : The Oxford Internet Institute (OII), 2005. Safety & Security in a Networked World: Balancing Cyber-Rights & Responsibilities.

7. *Guidelines for Best Practice in the Forensic Examination of Digital Technology.* **International Organization on Computer Evidence (IOCE).** Orlando : s.n., 2002. IOCE 2002 Conference.

8. **Daubert v. Merrell Dow Pharmaceuticals, Incharge.** 509 US 579 1993.

9. **Cohen, Frederick B.** Fundamentals of Digital Forensic Evidence. *Handbook of Information and Communication Security.* s.l. : Springer, 2010, pp. 789--808.

10. **National Institute of Standards and Technology.** Smart Phone Tool Specification. *Information Technology Laboratory, Computer Forensics Tool Testing Program.* [Online] 12 April 2010. http://www.cftt.nist.gov/documents/Smart_Phone_Tool_Specification.pdf. Version 1.1.

11. **US-CERT.** Computer Forensics. *US-CERT United States Computer Emergency Readiness Team.* [Online] 2008. [Cited: 10 February 2010.] http://www.us-cert.gov/reading_room/forensics.pdf.

12. *Computer forensics: the need for standardization and certification.* **Rogers, Meyers, Matthew and Marc.** 2, 2004, International Journal of Digital Evidence, Vol. 3, p. 2002.

13. *Defining digital forensic examination and analysis tools using abstraction layers.* **Carrier, Brian.** 4, s.l. : Citeseer, 2003, International Journal of digital evidence, Vol. 1, pp. 1-12.

14. *A ten step process for forensic readiness.* **Rowlingson, Robert.** 3, s.l. : Citeseer, 2004, International Journal of Digital Evidence, Vol. 2, pp. 1-28.

15. **Ashcroft, John.** Electronic Crime Scene Investigation A Guide for First Responders. *National Institute of Justice.* [Online] July 2001. [Cited: 2010 March 23.] https://www.ncjrs.gov/pdffiles1/nij/187736.pdf.

16. *A Road Map for Digital Forensic Research.* **Palmer, Gary.** Utica, New York : s.n., 2001. First Digital Forensic Research Workshop. pp. 27-30.

17. *An examination of digital forensic models.* **Reith, Mark, Carr, Clint and Gunsch, Gregg.** 3, s.l. : Citeseer, 2002, International Journal of Digital Evidence, Vol. 1, pp. 1-12.

18. *Getting Physical with the Digital Investigative Process.* **Spafford, Brian Carrier and Spafford, Eugene H.** 2, s.l. : Citeseer, 2003, International Journal of Digital Evidence, Vol. 2, pp. 1-20.

19. **Casey, Eoghan.** *Digital evidence and computer crime: forensic science, computers and the Internet.* s.l. : Academic Press, 2004.

20. *Computer Forensics--Past, Present And Future.* **Huebner, EWA, Bem, D. and Bem, O.** 2, 2003, Information Security Technical Report, Vol. 8, pp. 32-36.

21. **Jansen, Wayne and Ayers, Rick.** Guidelines on cell phone forensics. [Online] 2007. [Cited: 28 June 2010.] http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf.

22. **Yasinsac, Alec, et al.** *Computer Forensics Education.* s.l. : IEEE Security & Privacy, 2003. pp. 15-23. Vol. 1.