Annual ADFSL Conference on Digital Forensics, Security and Law

2008 Proceedings

Designing Laboratories for Small Scale Digital Device Forensics

Richard P. Mislan
Assistant Professor, Cyber Forensics Lab, Department of Computer & Information Technology, College of Technology, Purdue University, rmislan@purdue.edu

Tim Wedge
Computer Crime Specialist, NW3C, twedge@nw3c.org

Follow this and additional works at: https://commons.erau.edu/adfsl

Part of the Computer Engineering Commons, Computer Law Commons, Electrical and Computer Engineering Commons, Forensic Science and Technology Commons, and the Information Security Commons

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL

Designing Laboratories for
Small Scale Digital Device Forensics

Richard P. Mislan
Assistant Professor
Cyber Forensics Lab
Department of Computer & Information Technology
College of Technology
Purdue University
rmislan@purdue.edu

Tim Wedge
Computer Crime Specialist
NW3C
twedge@nw3c.org

ABSTRACT

The ubiquity of small scale digital devices (SSDD), the public's ever increasing societal dependence on SSDD, and the continual presence of SSDD at all types of crime scenes, including non-technical and violent crimes, demand a formalized curriculum for the education and training of future cyber forensic examiners. This paper presents the various SSDD forensics labs currently in use and under development for future use at the Purdue University Cyber Forensics Laboratory. The primary objective of each module is to provide specific real-world cases for the learning, comprehension, and understanding of hands-on investigative techniques and methodologies. The purpose of this paper is to outline those elements that will make effective Small Scale Digital Device Forensics labs.

Keywords: Forensics, Cyber Forensics, Digital Evidence, Education, Training, Small Scale Digital Devices, Personal Digital Technologies

1.0 INTRODUCTION

As Small Scale Digital Devices (SSDD) have become so pervasive in the daily social fabric of our lives, they have also presented a wealth of information for our forensic examiners. As personal storage units of all that is important to our social lives, these devices tell of who we know, who we communicate with, and what we find worth capturing.

As treasure troves, these SSDD are not easy "nuts to crack." Over the past ten years, the world of computer forensics has had the luxury of a limited handful of file system formats, being ensconced in forensic standards and systems developed to acquire and analyze these evidentiary hard drives. As SSDD forensics is still in its infancy, forensic examiners are still debating the standards and methods for acquiring these idiosyncratic devices (Ayers et al., 2007; SWGDE, 2007; Ayers et al., 2006; Gratzner, Naccache, Znaty, 2006; InterPol, 2006; McCarthy, 2005; ACPO/NHTCU, n.d.; IOCE, 2000).

2.0 SMALL SCALE DIGITAL DEVICES

By definition a Small Scale Digital Device is "a small form factor device which utilizes permanent or temporary memory in conjunction with embedded chips to perform a variety of tasks" (Harrill and Mislan, 2007). Categorically, SSDD have been further defined by the various types of devices:

- Personal Digital Assistants

- Cellular Telephones

- Audio / Video Devices

- Gaming Devices

- Other Devices

As the name suggests, SSDD are characterized by their physical size which appears to be diminishing over time. As these devices grow smaller, and more personal, they have extended functionalities storing massive amounts of information. Furthermore, many of these SSDD provide the means of synchronizing information to another computer, whether through wired or wireless networks such as WiFi or Bluetooth.

2.1 Personal Digital Assistants

In 1992, Jeff Hawkins spawned the beginning of the Personal Digital Assistant rage that ran well through the last part of the century. Soon after, names like Newton, Nino, Palm, iPaq, and Zaurus became handheld household names. Providing Personal Information Management (PIM) applications like calendars, contacts, task lists, and memo pads, these devices became the device du jour for the business world.

2.2 Mobile Telephones

In 1973, when Martin Cooper placed the first call on his "Brick Phone", a revolution started that has forever changed the social fabric of our daily lives. Mobile phones of today are so ubiquitous (Jansen, Ayers, 2006), that rather than just placing calls, these devices provide technologies for Short Message Service (SMS) messaging, Multi-Media Messaging Service (MMS) messaging, Instant Messaging (IM), electronic mail, Web browsing, multimedia capturing and playback, electronic document previewing, basic Personal Information Management (PIM) applications (e.g., contacts, calendar, etc.) and financial transactions (Willassen, 2003).

2.3 Audio/Video Devices

In 2001, Apple Computer started a revolution changing the face of the music industry overnight. With the birth of the iPod, a whole world of music lovers started "ripping" their CD collections to store on these portable music devices. Not long after the birth of the iPod, and many years after the beta vs. VHS wars, came the world of portable digital video players. Digital video players have become so prevalent thanks to products like Apple's Video iPod that it is not uncommon to carry entire seasons of syndicated television in one's pocket or purse. Unfortunately, today's criminals have also found that these large portable hard drives can store much more information than just music (Marsico and Rogers, 2005).

Finally, an overarching characteristic of SSDD is the variety of the different manufacturers, service providers, operating systems, technologies, form factors, and data and power cables. The combinatorial explosions that culminate from these various categories and characteristics of SSDD lend to a wide variety of physical and virtual possibilities (Gratzner, Naccache, Znaty, 2006).

3.0 FORENSICS OF SMALL SCALE DIGITAL DEVICES

In today's wired society, many crime scenes are littered with some type of digital evidence (Robinson and Smith, 2001). More times than not, crimes scene evidence is found on a thumb drive, a cell phone, or another type of SSDD. Unfortunately, first responders don't always realize the potential time-criticality and sensitivity of such digital evidence. With the ever-increasing storage capacitance and the ever-decreasing physical size of these devices, it is imperative to prepare our future forensic examiners and investigators with the tools and techniques for analyzing these evidentiary devices.

SSDD Forensics is the science of recovering digital evidence from SSDD under forensically sound

conditions using accepted methods (Harrill and Mislan, 2007). SSDD, especially those with advanced capabilities, are a relatively recent phenomenon, not usually covered in classical computer forensics (Jansen and Ayers, 2005). Thus, it has become a major initiative at the Purdue University Cyber Forensics Laboratory to create a SSDD Forensics course with representative labs.

As digital technology evolves, the existing capabilities of these devices continue to improve rapidly. When SSDD are involved in a crime or other incident, forensic examiners require tools that allow the proper retrieval and speedy examination of information present on the device (Jansen and Ayers, 2006). Unfortunately, these exist as a "Swiss Army knife" collection of tools from various manufacturers, open source groups, or underground, black hat, or hacker sources. As an endorsement of the "Swiss Army knife" approach, the Scientific Working Group on Digital Evidence (SWGDE, 2007) suggests the following procedure when examining Mobile Phones:

1. Use proven and validated hardware/software solutions. If the phone includes a SIM card, examine the card with and without the handset.

2. Use open source, free, or manufacturer-specific tools.

3. Use wireless transfer methods such as Bluetooth or Infrared.

4. Use the suspect device to display data while photographing or videotaping the screen.

5. Transcribe information viewed on the device to include call logs, phone books, text messages, etc.

6. Use the suspect device to E-Mail or forward the data to an examination device. In the event this method is used, the examiner must document why this method was used and the steps taken. The examiner must also ensure that the data received is an accurate depiction of what was on the suspect device.

As with cell phones, the multiple attempts of data acquisition work well with other types of SSDD. These multiple attempts are directly related to the multiple tools that the students are exposed to: DirSnoop, Access Data FTK, GSM .XRY, Cellebrite UME36, Secure View, Device Seizure, SIMCon, SIMIS, iDEN Companion Pro, iDEN Phonebook Manager, iDEN Media Downloader, Blackberry Desktop Manager, Amber Blackberry Converter, Oxygen Phone Manager, MobilEdit!, TULP2G, Nokia PC Suite, Sony Ericson PC Suite, various Flasher Boxes, several of our own developed tools, and various other data synchronization tools.

The main reason so many tools are necessary for SSDD forensics is that combinatorial explosion mentioned earlier. A good example of this is the Motorola RAZR cell phone. To date there are over twelve versions of this single phone, ranging from the RAZR V3 to the V9, each with its own technological modifications. Beyond the minor form factor variations, the manufacturer, Motorola, has recently changed the data/power connection from Mini USB to the newer Micro USB standard (Open Mobile Terminal Platform, 2007). To add to this, each network service provider adjusts the operating system or application software to their specific needs. Beyond this, a user may implement changes specific to their personal preferences. With so many variables, it makes this field of forensics ever-so dynamic, with a challenge at every turn (McCarthy, 2005; Robinson and Smith, 2001).

3.1 Lab Modules

To prepare our students for our reality and their future, we have designed real-world forensic labs based on cases taken from the headlines or various examiners experiences. The details are well developed and the actual devices, tools, and techniques are used throughout the forensic acquisition, preservation, analysis, and presentation of each case.

Currently, we are working with five labs: a murder, a kidnapping, a meth lab, corporate IP theft, and military intelligence gathering. Each lab is unique including at least ten different individuals, background case information, details about the suspects and victims, and at least five small scale

digital devices. Each of these devices includes evidence that can either help or hurt the investigation. In some instances, the evidence may point the students towards the Internet, leveraging information (either planted or previously existed) to further their investigations.

The goal for each of these labs is to take the students from cradle to grave of an actual investigation, learning how to process each type of SSDD evidence using the actual forensic tools and techniques that may or may not support these devices. This is not only about learning the proper techniques to handle, acquire, analyze, and present the evidence, but also how to determine if the newly found information is useful or not. The added elements of realism and surprise provide for an ever-engaging and thought-provoking environment.

In each lab, students are presented with multiple SSDD, all interacting with each other at various levels. One unique case is the Meth Lab Explosion, which revolves around the remnants of a Meth Lab, several badly burned victims, and several suspects who may or may not have been involved in the activities which led up to the explosion. Given this scenario, the devices found on the scene include the melted thumb drive, charred cell phone, and its SIM card. Other evidence collected from the suspects includes the Blackberry and two iDEN phones.

The SIM Card was found in the charred cell phone, which was still in the hand of a young college girl who died in the horrific explosion. Also found at the scene was a melted thumb drive in the pocket of another young college boy. With the SIM Card alone, the students are possibly able to determine who she knew, who she had been communicating with (SMS, MMS), and who she might have been called last. The thumb drive may have files related to the activities of the event or may be totally unrelated. The Blackberry and the iDEN phones are related to the accident, but are from suspects who escaped or were not present at the explosion. Ideally, these devices will also provide further information for the investigation or lead to dead ends.

4.0 EDUCATIONAL CONSIDERATIONS & EXPECTATIONS: CONTROLS AND VALIDATION

4.1 Validation in the Absence of Hashing

The nature of many of these devices often precludes the use of hashing as a validation method.

There remains a need to establish reliable methods for verifying what data was placed on the device pre-seizure, and that (preferably) no data was placed on the device post-seizure or, if data was placed on the device (due to practical constraints) the report includes comprehensive documentation explaining why, and placing a verifiable boundary on what data could and could not have been altered. Specific methods will vary from device to device, but instilling the necessity into the minds of future examiners is an important element in the development of lab exercises.

4.2 Use of Known Values

"How do you know if you've found all the evidence?" "How do you know if everything you've found is evidence?" These are questions that have plagued analysts for years, particularly in the field of digital recovery. In real life, it is usually impossible to answer these questions with certainty. In a training environment, it is imperative that students receive timely feedback to determine that the procedure they used was successful or not successful. There is a strong risk that ineffective or, worse, partially effective classroom techniques will carry over into on the job practices down the road. The specifics vary widely, but generally take one of two forms:

(1) The instructor inserts known values (which are unknown to the students) into piece of media and the student has to apply learned techniques, and ideally, some creative problem solving to find these values. Generally, this is a device that is being treated and handled as simulated evidence. This enables the instructor to reliably measure the degree of success of the students' evidence handling and processing methodologies as well as their interpretation of results.

(2) The student takes predetermined steps using noted values and then uses learned techniques and tools to observe the actual results. Because this involves actual changes to the device, this form is limited to devices that are NOT being treated as simulated evidence in the lab. This has the advantage of allowing the student to gain a greater understanding of the "cause and effect" relationship between a variety of user actions, and the digital artifacts that are created as a result of those actions.

4.3 Investigative Roles and the Big Picture

The process of retrieving useful information from a device and placing it in evidentiary context involves multiple roles (Ayers, Jansen, Cilleros, and Daniellou, 2006). Over the course of a semester, students are rotated through as many of these roles as possible as each simulated case is processed. This not only gives the student the experience of that role, but in dealing with the interactions between the roles as well. Full implementation of all roles in every exercise will not always be practical or necessary, and the emphasis in most cases will be on the role of the examiner. The typical "flow" of the ideal process will follow the steps outlined in Figure 1 below:
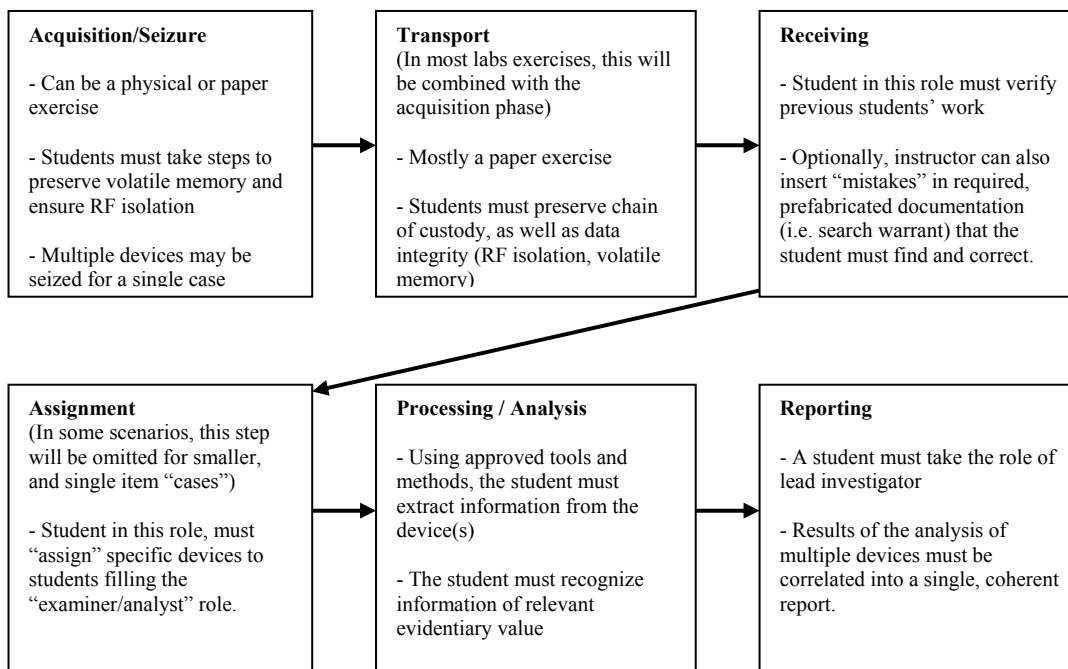
Acquisition/Seizure - Can be a physical or paper exercise - Students must take steps to preserve volatile memory and ensure RF isolation - Multiple devices may be seized for a single case	Transport (In most labs exercises, this will be combined with the acquisition phase) - Mostly a paper exercise - Students must preserve chain of custody, as well as data integrity (RF isolation, volatile memory)	Receiving - Student in this role must verify previous students' work - Optionally, instructor can also insert "mistakes" in required, prefabricated documentation (i.e. search warrant) that the student must find and correct.
Assignment (In some scenarios, this step will be omitted for smaller, and single item "cases") - Student in this role, must "assign" specific devices to students filling the "examiner/analyst" role.	Processing / Analysis - Using approved tools and methods, the student must extract information from the device(s) - The student must recognize information of relevant evidentiary value	Reporting - A student must take the role of lead investigator - Results of the analysis of multiple devices must be correlated into a single, coherent report.

Fig. 1: Flow of Forensic Process

4.4 Establishing Goals and Objectives

On the surface, the requirement is deceptively obvious. As discussed earlier, the evidence to be found consists of known values, evidence handling procedures are standardized, and must be adhered to. Furthermore, the end result is supposed to be the concrete identification of a single individual to be held culpable for the commission of a defined illegal act. It is tempting, therefore, to see the process as some kind of flowchart with correct and incorrect steps to follow, or as a series of yes/no questions, with corresponding right and wrong answers that can be objectively graded the same way every time. This in turn, can easily draw the instructor to treat the process as a demonstration of the "application" category of the cognitive domain (Anderson, et al, 2001) where the student need only follow the correct steps every time to achieve success. Giving into that temptation would leave the student woefully unprepared for "the real world" and ignores several factors critical to the successful handling, reporting and presentation of digital evidence.

It is important to remember that while certain steps and procedures must always be observed regardless of the circumstances, there remain many variables that render a pure "flow chart process"

approach to investigation generally ineffective. The type of crime or suspected activity varies from case to case. Technical considerations also vary widely from case to case, the number and type of evidence items, the services that the suspect(s) or other related parties may or may not have used, their relation ship to alleged activities all vary widely. Active attempts by investigative subjects to remove potential evidence will affect not only the results of the process, but the actual steps of the process.

The students' work product is, in fact, a synthesis, and can often require a great deal of creativity. Students must not only use a tool correctly, but must first evaluate a variety of factors in selecting the correct tool to use. Throughout the process, the students must repeatedly form hypotheses, and must then devise and perform tests for each (or correctly recognize when a hypothesis cannot be tested with available evidence or resources).

Even though the simulated evidence may have been prepared, and 100% of the evidence artifacts a known factor to the instructor, it is not always reasonable to use the number of specific items found and recorded as a standard to measure success. It is not generally feasible for every potential digital artifact to be manually evaluated, and more than one path may lead to a correct, verifiable conclusion. We cannot hold the student to a standard that would be unachievable in the field.

It remains that there must be a "right answer", and it must be correct and objective. It must be clear when the student has succeeded, and just as clear when the student has not. There are objective elements to a successful examination. Success of the examination can be determined by looking at these elements in the context of the specific case scenario. These elements include:

- Was the case solved? Was a correct conclusion reached? To be considered successful the evidence and its analysis should clearly show that an identified individual is the guilty party to such a degree that no reasonable person would disagree with the conclusion.

  ***Note that this does not necessarily require that every digital artifact on a device be the subject of human analysis.

- Were forensically sound procedures followed throughout the process? Was any evidence altered or lost as a result of the evidence handling or processing?

- Were the hypotheses formed reasonable? Were the tests devised to test those hypotheses effective and correctly executed and interpreted?

- Did the student reach and state conclusions that are not supported by the evidence found (regardless of the factual correctness of the conclusion)? Was there any misinterpretation of the evidence?

- Did the student look in reasonable appropriate places for both incriminating and exculpatory evidence?

5.0 CONCLUSIONS AND FUTURE PLANS

To build these labs, we have built up quite an extensive inventory of SSDD. On campus we worked with our telecommunication office to offload their inventory of old or broken phones and PDAs. In the community we worked our local Women's Shelter and continually help them sort through their incoming inventory of donated phones. Globally, we are working with several recycling companies to increase our library of cell phones. To date, we have built up a collection of over three hundred unique SSDD and are currently in the development of a forensic acquisition tool testing database and a SSDD forensics knowledge base, providing a needed resource for federal, state, and local law enforcement forensic examiners.

In addition to gathering more equipment, we are also looking forward to additional forensic labs. The

current plans are to incorporate other devices such as portable gaming devices, handheld GPS systems, VOIP and satellite phones, and carputers. Additionally, other features we might add include practical exercises for accessing obstructed (password protected) devices. The one thing we can count on in this field is that the memory capacitance will increase, and the device will get smaller.

AUTHOR BIOGRAPHIES

Richard Mislan is an Associate Professor of Computer and Information Technology at Purdue University, West Lafayette, Indiana. His research interests include Small Scale Digital Device (SSDD) forensics, unusual sources of digital evidence, and the application of artificial intelligence techniques for improving efficiency in cyber forensics. He can be reached at rmislan@purdue.edu.

Tim Wedge has the dual role of Computer Crime Specialist at the National White Collar Center, based in Glen Allen, Virginia and Research Scientist at Purdue University, West Lafayette, Indiana. His research interests include improved tool validation methodologies, and the development of tools for improving accuracy and precision in cyber forensics. He can be reached at twedge@nw3c.org.

REFERENCES

Anderson, L., Krahtwohl, D., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., Raths, J., Wittrock, M, (Eds). (2001) *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*. Addison Wesley Longman

Ayers, R., Jansen, W., Cilleros, N., Daniellou, R. (2006). An Overview of Cell Phone Forensic Tools. Retrieved on Sept. 10, 2007 from http://www.techsec.com/TF-2006-PDF/TF-2006-RickAyers-MobileForensics-TechnoForensics.pdf

Ayers, R., Jansen, W., Cilleros, N., Daniellou, R. (2006). Cell Phone Forensic Tools: An Overview and Analysis. Retrieved on Sept. 12, 2007 from http://csrc.nist.gov/publications/nistir/nistir-7250.pdf

Ayers, R., Jansen, R., Moenner, L., Delaitre, A. (2007). Cell Phone Forensic Tools: An Overview and Analysis Update. Retrieved on Sept. 10, 2007 from http://csrc.nist.gov/publications/nistir/nistir-7387.pdf

Gratzner, V., Naccache, D., Znaty, D.(2006). Law Enforcement, Forensics and Mobile Communications. Retrieved on Sept. 10, 2007 from

http://www.cl.cam.ac.uk/~fms27/persec-2006/goodies/2006-Naccache-forensic.pdf

Harrill, D., Mislan, R. (2007). A Small Scale Digital Device Forensics ontology. Retrieved on August 30, 2007 from http://www.ssddfj.org/papers/SSDDFJ_V1_1_Harrill_Mislan.pdf

Interpol Mobile Phone Forensic Tools Sub-Group. (2000). Good Practice Guide for Mobile Phone Seizure & Examination. Retrieved Sept. 10, 2007 from http://www.holmes.nl/MPF/Principles.doc

IOCE. (2000). Good Practices for Seizing Electronic Devices - Mobile Telephones. Retrieved Sept. 10, 2007 from http://ncfs.org/documents/ioce2000/reports/electronicDevices.pdf

Jansen, W., Ayers, R. (2006). Forensic Software Tools for Cell Phone Subscriber Identity Modules. Retrieved Sept. 10, 2007 from http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_forensics/JDFSL-proceedings2006-fin.pdf

Jansen, W., Ayers,R. (2007). Guidelines on Cell Phone Forensics. Retrieved Sept. 10, 2007 from http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

McCarthy, P. (2000). Forensic Analysis of Mobile Phones. Retrieved Sept. 10, 2007 from http://esm.cis.unisa.edu.au/new_esml/resources/publications/forensic%20analysis20of%20mobile%20phones.pdf

Marsico, C., Rogers, M. (2005). iPod Forensics. Retrieved November 3, 2006 from https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2005-13.pdf

Open Mobile Terminal Platform. (2007). Broad Manufacturer Agreement Gives Universal Phone Cable Green Light. Retrieved on January 11, 2007 from http://www.omtp.org/news/news_pr_universal_cable.html

Robinson, G., Smith, G. (2001). Evidence from Mobile Phones. The Legal Executive. Journal of the Institute of Legal Executives. Retrieved on September 12, 2007 from http://www.ilexjournal.com/special_features/article.asp?theid=284&themode=2

Willassen, S. (2003). Forensics and the GSM Mobile Telephone System. International Journal of Digital Evidence, Spring 2003. Volume 2, Issue 1.