On Integrating Mobile Applications into the Digital Forensic Investigative Process

April Tanner, Ph.D.
Department of Computer Science
Jackson State University
Jackson, USA

Soniael Duncan
Department of Computer Science
Jackson State University
Jackson, USA

***Abstract*— What if a tool existed that allowed digital forensic investigators to create their own apps that would assist them with the evidence identification and collection process at crime scenes? First responders are responsible for ensuring that digital evidence is examined in such a way that the integrity of the evidence is not jeopardized. Furthermore, they play a pivotal part in preserving evidence during the collection of evidence at the crime scene and transport to the laboratory. This paper proposes the development of a mobile application that can be developed for or created by a first responder to assist in the identification, acquisition, and preservation of digital evidence at a crime scene.**

Keywords—mobile device forensics; digital forensics; forensic process, forensic models; MIT App Inventor

I. INTRODUCTION

Digital Forensics involves the identification, preservation, collection, examination, and analysis of digital devices. These devices include, but are not limited to, digital cameras, flash drives, computers, internal and external memory drives, mobile devices, etc. Some mobile devices that can be examined include graphic tablets, cell phones, smart phones, CDs, DVDs, and MP3s. Digital evidence has to be collected under certain parameters as to maintain the integrity of the investigation. This process is referred to as a forensic process. While there is not a concrete set of rules for the forensic process there are models that have been proposed to aid in trying to eliminate damage and contamination that can occur at crime scenes.

This paper identifies the types of damage and contamination that can occur at crime scenes when inexperienced first responders arrive at the scene; in addition, we discuss the models that address the preservation and acquisition of evidence at crime scenes, and also explore possible solutions to aid first responders in utilizing techniques to preserve digital evidence at the scene of the crime. In this paper, we propose the development and implementation of a mobile application that first responders can create and use as a guide when identifying, preserving, collecting, and securing evidence. As a result, this application would be useful in assisting first responders during the acquisition process of a digital forensics investigation.

II. BACKGROUND

In the 21st century, computer crimes have become more of a concern than in past years. The advancement of technology has led to the advancement of crime, such that there is now a need for various methods of evidence collection. Traditionally, physical evidence was collected from a crime scene. Due to the elevation of technology and the rise of digital devices, many of these electronic devices are used in criminal activity. The United States Department of Justice (USDOJ) created a table that categorizes types of crimes and types of evidence associated with those crimes. In Fig. 1, in the sex crime category, where prostitution is being investigated, an investigator should check databases, e-mail, notes, letters, financial/asset records, medical records, address books, calendar, and customer database/records to retrieve evidence [8]. Forensic analysts and investigation teams are responsible for obtaining evidence of this magnitude; however, first responders are often responsible for identifying and collecting devices that this evidence may reside in.

During investigations, first responders are initially deployed to the scene of a crime. First responders, who may or may not be trained forensic examiners, may have dual roles in an investigation. Many times they are untrained in the areas of digital forensic evidence collection and digital crime scene preservation which are vital to any digital forensic investigation. At this point, errors would lead to contamination of evidence and the integrity of the investigation would become compromised or deemed invalid for submission in court proceedings. As the age of computers and technology increase and advance, the crimes committed, where digital devices are involved, will also evolve in type, complexity, and damage perimeter. Thus, the forensic process of digital devices has to be as thorough and concise as possible to protect against viruses, worms, malware, and other possible cyber attacks.

The USDOJ created a forensic process model that guides first responders to help them better assess crime scenes upon initial response. They stated that "the process of collecting, securing, and transporting digital evidence should not change the evidence, digital evidence should be examined by those trained specifically for that purpose, and everything done during seizure, transportation, and storage of digital evidence should be carefully documented, preserved, and available for review" [8]. Their model consists of four phases: collection, examination, analysis, and reporting. First responders are primarily responsible for the collection of evidence at the crime scene. The collection phase is described as the phase in which the search, seizure, and documentation of evidence takes place [1].

We would like to acknowledge the Department of Energy/National Nuclear Security Administration for providing funding for this research under Dr. Samuel P. Massie Chairs of Excellence Grant#: 240946.

There are a number of other models that have been created and proposed as well [1, 4]. First Responders have to be careful in their seizure of digital evidence because if it is handled improperly it could violate the Electronic Communications Privacy Act of 1986, the Privacy Protection Act of 1980, and federal laws [8]. As a result, researchers have proposed different types of models that provide a more in depth analysis to how a first responder should identify evidence, collect it, and preserve the crime scene until the appropriate forensic teams are deployed to continue the investigation [1, 2, 4, 8].

Fig. 1.1 displays information regarding evidence first responders should collect [8]. These tables created by the USDOJ, categorize the types of evidence one should look for or investigate depending on the type of crime. For example, if it is a sex crime that involves child exploitation/abuse an investigator should investigate e-mail, notes, letters, chat logs, date and time stamps, digital cameras, software, and images [8].

Forensic process models are useful in assisting with breaking down the phases into specific and less ambiguous tasks that will aid in gathering evidence located at any crime scene. The Abstract Digital Forensics Model breaks these two phases into five phases: Identification, Preparation, Approach Strategy, Preservation, and Collection, which first responders are responsible for [1]. These stages merely suggest that first responders identify the type of incident that has occurred, prepare all necessary tools and techniques, and obtain proper authorization to proceed with evidence collection, create a strategy to approach collecting the evidence without tainting it, preserve the state of the evidence whether it is digital or physical, and collect the evidence using proper forensic procedures. These phases require that, during evidence collection, evidence should be authenticated and valid for court proceedings.

Additional models exist that suggest that there is more to be evaluated and there are some models that seem to eliminate the first responder or merely suggest that first responders become trained in forensically sound evidence collection. In most cases, first responders, investigators, and examiners have little or no knowledge of digital forensic process models. Generally, these individuals acquire evidence at the scene based on general evidence collection procedures and/or training from a colleague, in which, the evidence information is documented using paper-based methods. In this paper, we propose the development of a mobile application that can be used as a guide for collecting digital evidence at a crime

	Sex Crimes			Crimes Against Persons			Fraud/Other Financial Crime						
	Child Exploitation/Abuse	Prostitution	Death Investigation	Domestic Violence	E-Mail Threats/ Harassment/Stalking	Auction Fraud	Computer Intrusion	Economic Fraud	Extortion	Gambling	Identity Theft	Narcotics	Software Piracy	Telecommunications Fraud
General Information:														
Databases		✓				✓		✓		✓				
E-Mail/notes/letters	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Financial/asset records		✓	✓	✓	✓	✓		✓		✓		✓		✓
Medical records		✓	✓	✓										
Telephone records			✓	✓	✓	✓								✓
Specific Information:														
Account data						✓								
Accounting/bookkeeping software						✓								
Address books		✓	✓	✓	✓	✓	✓	✓		✓		✓		
Backdrops										✓				
Biographies			✓											
Birth certificates										✓				
Calendar		✓				✓		✓			✓			
Chat logs	✓					✓						✓		
Check, currency, and money order images							✓			✓				
Check cashing cards										✓				
Cloning software														✓
Configuration files						✓								
Counterfeit money										✓				
Credit card generators										✓				
Credit card numbers										✓				
Credit card reader/writer										✓				
Credit card skimmers							✓							
Customer database/ records		✓						✓						✓
Customer information/ credit card data						✓		✓						
Date and time stamps	✓								✓					
Diaries			✓	✓	✓									
Digital cameras/software/ images	✓					✓				✓				
Driver's license										✓				
Drug recipes											✓			
Electronic money								✓						
Electronic signatures										✓				

Fig. 1. Snapshot of USDOJ evidence targets by case category [8]

scene. Using simple, easy-to-learn tools, the application could also be developed by a trained investigator to use to train novice first responders, or it could be developed by the novice first responder himself. This mobile application will serve as a tool to guide first responders, whether trained or untrained, in maintaining the integrity of digital evidence while collecting digital evidence during an investigation. No previous work was found that used the MIT App Inventor software to create an application to assist in the digital forensic investigation process.

III. Design and Implementation

The ideas for this application stemmed from a lawyer who suggested the creation of a mobile application that would help professional investigators collect and authenticate evidence using an Android device. According to the lawyer, the Android device should have the dual camera (front and back cameras) capability. Features the application should possess included the following: 1) The ability to snap a photo with outward-facing (back) camera; 2) The ability to launch the

user-facing (front) camera to collect video of the first responder at the scene; and 3) To provide scripts for user to say on video to authenticate the attached photos and any evidence collected. Based on the template provided, we modeled a portion of the mobile application's design after the suggested features [6].

The proposed mobile application could be used as a guide for first responders in digital forensic evidence collection. This application would not only provide instructions for evidence identification but could also provide tips and suggestions for evidence collection. The application would have email, web, video, camera, voice and sound features. It would also allow a first responder to record their identity and authenticate their investigation through the photo and video capabilities, access the internet to send secure emails of any of the photos or videos that have been taken, and store any contacts or information that may be needed. This fully functioning application would also have instructions for evidence collection embedded in buttons. This application is an ongoing project and additional modifications are currently in progress.

MIT App Inventor is software originally created by Google Labs for Google engineers and Google users interested in simplified mobile application creation and development [5, 7]. This software is freely available to the public for use. The software is used as a canvas for mobile app design and provides a foundation for inexperienced and experienced programmers. User created MIT App Inventor applications can range from simple games to complex apps that educate and inform. MIT App Inventor's text to speech capabilities allows the phone to ask questions aloud. To use MIT App Inventor, you are not required to be a professional coder. This is because instead of writing code, you visually design the way the application looks and use blocks to specify the application's behavior. MIT App inventor does not require an extensive knowledge in Java programming because the programming aspect is like a puzzle [7]. There is not any necessary hard coding required, the block editor allows the developer to piece the "code" together and then test the functionality of the app through the software's emulator [5, 7].

Figures 1.2 and 1.3 show the components created using MIT App Inventor that provides this application's functionality.

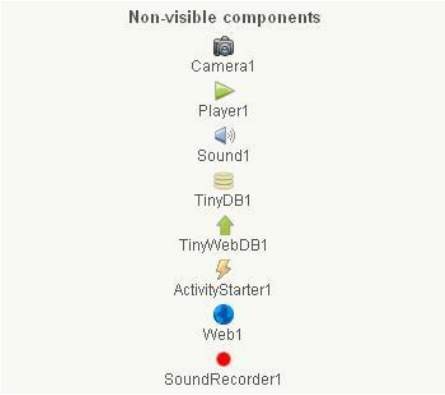

Fig. 2. MIT App Inventor non-visible components [7]

Fig. 2. MIT App Inventor visible components continued [7]

In Fig. 1.2, the non-visible components are not seen on the applications home screen but are still included in the application's functionality. Some of these components are self-explanatory while others are linked together to perform a function. For example, the player1 component allows audio and video to be played and controls the phone's vibration. The tinyDB1 components are storage components that allow the user to retrieve and store information to the phone [7]. These components are helpful to the forensic investigation process because all the information taken can be stored to the device's memory without risk of losing any evidence collected. An application of this magnitude allows a first responder to pause their investigation at any point without losing any of the evidence or data they have obtained. Some applications have to have web access to operate. This application would not require web access to function but would have web capabilities in case a first responder needed to find the type of model of a digital device left at the scene of a crime. This application is designed to operate on Android mobile devices that have dual camera capabilities; however, at the time of development, the MIT App Inventor software did not provide that component. If an Android mobile device has a camera, the application can still run. While they may not be able to have dual camera functionalities, a sound recorder has been implemented in the application's design to allow the first responder to identify themselves and record any information necessary to the investigation. This tool is not designed to be restricted to cell phone usage only. Graphic tablets such as the Samsung Galaxy, Toshiba Thrive, and other devices that use the Android OS software can access it.

Fig. 1.3 depicts the app inventor emulator with some of the mobile application functions provided on the home screen. The sound recorder would also list the tasks to be completed based on the model phases previously presented. Embedded in the picture with the magnifying glass is a recorded sound that instructs a first responder as to the information they need to provide to authenticate their identity. We discovered in development that a sound recorder would need to be added as well to accommodate those devices not equipped with front and back (dual) camera capabilities. Therefore, a sound recorder and a note pad were added to the apps functions. Google app inventor labs allows mobile app development to be created through the blocks editor, which allows inexperienced or beginner programmers to experiment with application development and a simpler type of coding.

The Blocks Editor component of the app inventor software is used for visually programming the application by fitting the pieces of those blocks together sort of like a coding puzzle as shown in Fig. 1.4 [7]. The software itself will let you know if you are coding incorrectly. Additionally, the software is equipped with programming capabilities for those who have experience in Java programming. Future goals are to enhance this application by providing the user with the ability to link to web pages that have information about evidence collection process on them and explain how to identify the types of evidence for the type of crime. Resultantly, this application could serve as a guide for first responders and also an evidence tool in the law enforcement community.

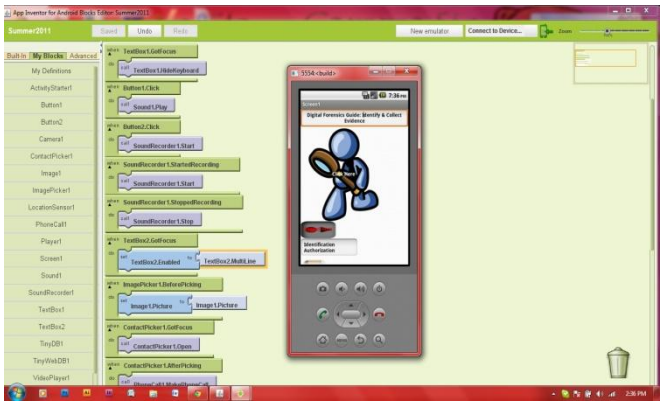

Fig. 3. App Inventor Block Editor and Emulator for the app

IV. Testing Phase

Testing the tool involved numerous trials resulting in some improvements in the applications development as well as some limits in the app inventor software. At the time of testing, some of the application's capabilities are not supported by the app inventor software and does not transfer very well to an actual cellular device. Some hard coding using logic and Java or JavaScript could possibly solve this problem however; extensive work on the app is required. During the testing phases, we discovered that the emulator accurately showed how the application functioned on a mobile device. At the time of development, some of the bugs in the web component were currently undergoing construction, and the software did not provide for the notebook capability which allowed attaching comments to a photograph. These are some of the limitations that were presented during testing phases.

Although problems were encountered in the application, some of the original components did function properly. The figures below depict the applications capabilities thus far.

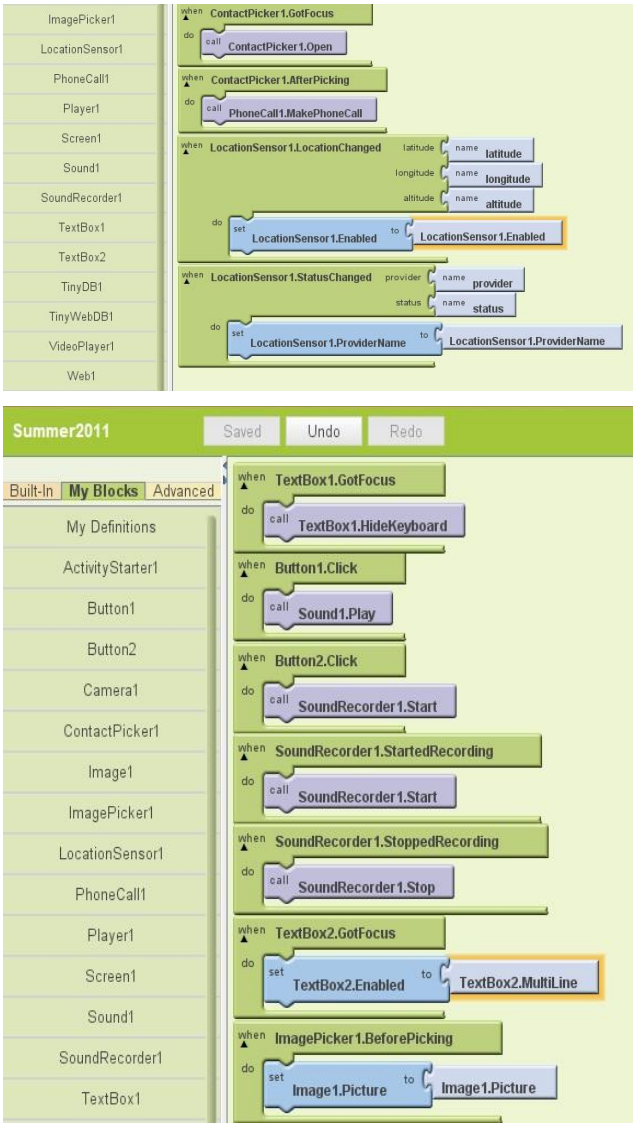

Fig. 4. MIT App Inventor Blocks Editor

Fig. 1.5 depicts the emulator in the app inventor software using the multi-line note pad capability of the app. During development and testing, it was found that this feature did not allow the user to connect comments to actual digital media (pictures, video, etc). Comments on pictures were not permitted by this application at this stage of development. Ideally, the user would be able to type comments associated with the picture that they have selected to view. Attempts to integrate this feature are ongoing at this time. In our continuous development efforts, we plan to address and correct this issue.

Fig. 5. App Inventor Emulator displaying the entering of evidence notes

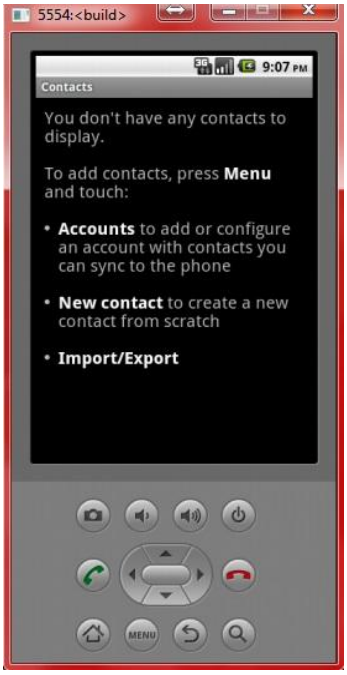

Fig. 6. MIT App Inventor Emulator displaying stored contacts

Fig. 1.6 shows the contacts feature of the application working properly. If the user clicks the contacts button it will link to whatever contacts are stored of the mobile device. The emulator did not show any contacts in the figure because there were not any stored on the device. However, it did perform correctly with the contacts when they were added.

Fig. 7. MIT App Inventor Emulator displaying app selections

Fig. 1.7 depicts the photo gallery feature of the mobile application as a functioning component. The figure depicts all the images related to this mobile app and other pictures downloaded and stored in a folder pertaining to mobile application design. While the emulator only shows those images in the folder, testing showed that the gallery function linked to the mobile phone's photo gallery and allowed pictures to be stored.

V. CONCLUSIONS

In this paper, we discussed the importance of documenting digital evidence at the crime scene, we identified the different types of incidents that could occur when first responders arrive at the scene, and we discussed why a mobile application would be useful in the evidence identification and collection of first responders. Little or no research has been found that discussed how mobile applications could be used to assist first responders in the evidence identification, collection, and documentation process. Therefore, in this paper, we attempted to develop a mobile application that could assist first responders in their digital investigations. However, the tool is currently undergoing modifications. Furthermore, it could still be developed into a powerful training tool that could be used by law enforcement and other investigative teams during an investigation.

During the development of the digital forensics application, Google App Inventor was used. MIT recently began hosting Google's App Inventor, which is now MIT App

Inventor in March 2012 [7]. Most of the design and experimentation performed prior to March 2012, shows that some of the components of the initial design were not supported by the Google App Inventor Emulator or software at the time of development. For example, we embedded a web viewer and email function in the application's initial design but testing has shown us that these functions are not supported by Google App Inventor's Emulator. This mobile application can be extended to include modifications, additional functionalities, and testing with real investigators. It could provide mobility and a succinct, electronic way of storing and documenting evidence acquired at the crime scene. It could also be modified to implement each of the phases of the digital forensic process to aid investigators during the analysis, reporting, and presentation phases. Given the simplicity of the tool, investigators could develop their own custom applications, for no cost to them, based on their individual needs. This application could be used as a basis for creating other versions of this application as well. The applications could be modified to include games, which provide different scenarios/crime scenes, for novice first responders to enhance their evidence identification and recovery skills.

Given the increase in digital crimes and the need for skilled digital forensic investigators, the development of such a tool is needed. Law enforcement officers generally do not have the time or funds to engage in training, especially with training on new digital tools. Developing a mobile application that can assist first responders in maintaining the integrity of the evidence and documenting the evidence "in real-time," benefits not only the first responders, but the entire law enforcement community.

VI. FUTURE WORK

Future enhancements to this work include linking a notepad and email function to the photo gallery to allow comments to be written associated with the photos and securely encrypted and emailed and stored on that organization's servers. Also, the bugs in the web viewer could be deciphered to allow email functionality and web browsing capabilities. An additional function to be added to the application is the implementation of a sound recorder that could be embedded in the application or link to a phone that allows voice recording to support those Android phones that are not dual camera capable. These additional enhancements to the application would make it both a useful and beneficial digital forensic investigation tool.

REFERENCES

[1] A. Tanner and D. Dampier, "An approach for managing knowledge in digital forensic investigations," International Journal of Computer Science and Security, vol. 4, no. 5, pp. 451-465, December 2010.

[2] F.C. Dancer, D. Dampier, J. Jackson, N. Meghanathan, "A theoretical process model for smartphones," Proceedings of the Second International Conference on Advances in Computing and Information Technology (ACITY), July 2012.

[3] R. P. Milsan, "Cell phone Crime Solvers: Could the murder victim's Blackberry lead to her killer?" IEEE Spectrum, July 2010.

[4] A. Ramabhadran, Security Group, and T. Elxsi, "Forensic investigation process model for Windows mobile devices," http://www.forensicfocus.com/downloads/windows-mobile-forensic-process-model.pdf, 2012.

[5] Google Labs, "App Inventor for Android," https://code.google.com/p/app-inventor-for-android/, 2011.

[6] App Inventor Coffee Shop, "Inspiration for a useful, even marketable,

[7] app," 2010.

[8] MIT App Inventor, "Explore MIT App Inventor," http://appinventor.mit.edu/explore/, 2012.

[9] A. Tanner, " A concept mapping case domain modeling approach for digital forensic investigations," doctoral thesis, Department of Computer Science and Engineering, Mississippi State University, Mississippi State, MS, 2010.