2012 3rd International Conference on e-Education, e-Business, e-Management and e-Learning
IPEDR vol.27 (2012) © (2012) IACSIT Press, Singapore

Development of an Application Program to Help Evidence Preservation by Using an Android Mobile Phone

Wataru Takahashi[†], Ryoichi Sasaki[†], Tetsutaro Uehara[%]

[†]Tokyo Denki University, 2-2 Kanda Nishiki-Cho, Chiyoda-ku, Tokyo 101-8457, Japan
[%]Kyoto University, Yoshida-Honmachi, Sakyo-ku, Kyoto 601-8501, Japan

Abstract. The need for digital forensics, which is the technique of preserving evidence and investigating and analyzing electronic records, has been increasing, since society depends greatly on information and communication technologies, and especially since disputes at various levels occur between individuals and organizations. The digital forensic operations performed by the people in charge of computer centers at the time of the first recording are not easy. To handle this problem, the Digital Forensic Institute in Japan developed a guideline to preserve the evidence of electronic records. However, it is not easy for individuals to keep evidence without a computer aid, because of the volume of records demanded by the guideline. Therefore, to easily transmit the guideline, we developed a system consisting of a GST (guideline support tool) in PCs for the authors of guidelines and a BTG (browsing tool for guidelines) for workers using an Android phone. The output of the GST can be used to illustrate the guideline automatically by the BTG on an Android phone.

Keywords: Digital Forensics, Information Security, Android, Support Tool, Preservation of Evidence

1. Introduction

The need for digital forensics, which is the technique of preserving evidence and investigating and analyzing electronic records, has been increasing, since society greatly depends on information and communication technologies, and especially since disputes at various levels occur between individuals and organizations [1]. Therefore, the digital forensic operations must be performed by the people in charge of computer centers to keep the evidence at the time of the first recording. The following two questions arise in the maintenance of this electronic evidence.

- Should we acquire the electronic record and across what range of electronic record?
- How should we guarantee the original identity of evidence to maintain?

Because Japan has a short history in digital forensics, no standard guidelines of widely recognized acquisition procedures exist. Therefore, the Digital Forensic Institute was created to handle this situation. One of the authors of this paper developed a guideline to preserve the evidence of electronic records [2]. However, because this guideline exceeds 20 pages (in A4 form), it is not easy for individuals who needs to preserve evidence in an emergency to react appropriately. In addition, the creation of guidelines places a burden on those who develop and modify the guidelines.

Therefore, we developed a program for a guideline system using Android phones. We also developed a support system to produce guidelines easily and a function to automatically transform data of guideline from the support system to programs on Android phones.

Although many types of studies on digital forensics [3][4] have been conducted, we have not been able to find other research that has developed a program that supports the guidelines of digital forensics.

2. Guideline to Keep the Evidence of the Electronic Record

2.1. Overview of the Guideline

The guideline developed by the Digital Forensic Institute to keep the evidence of an electronic record is a standard guideline. The content of this guideline includes the following:

- Preparations to perform beforehand
- Response to an incident after an outbreak
- Collection of physical objects, acquisition of physical objects, maintenance of physical objects
- Preparation of devices to keep evidence
- Preservation of evidence during and after preservation

2.2. Problem of the Guideline

The following problems exist for guideline users, such as the operator of a computer center, to preserve the evidence of an electronic record at the time of the first recording in an actual situation.

- Because the guideline to keep the evidence of an electronic record is more than 20 pages (A4 paper), initiating an immediate response using the guideline is very difficult and tedious.
- The people who wrote the guideline do not receive confirmation of whether the description is easy to carry out.

3. Proposed Method

To resolve the above problems, we decided to develop tools to support comprehensively not only the workers who keep the evidence of the electronic record but also the people who write the guideline.

3.1. Overview of the Proposed Method

A tool for workers, named the BTG (browsing tool for guidelines), was developed to keep the evidence of an electronic record on an Android phone. The reasons for using an Android phone are as follows.

- Compared to a PC, an Android phone is easy to carry when an incident occurs.
- Android phones are available as standard features for shooting the video and still images that are required to preserve evidence.
- Unlike iPhone applications, an Android application can be developed not only on a Mac OS but also on a Windows OS.
- Also, unlike iPhone applications, which are developed with the original development language, ObjectC, Android applications can be developed with Java language.

It is desirable to create a program that works automatically on an Android phone to enable workers to keep the evidence of the electronic record, even if no one is skilled in the guideline program. Since we knew that the guideline can be expressed as a mind map, we also developed a tool named the GST (guideline support tool) to generate application data to show the display for an Android phone from the guidelines described with the mind map [5]. Although the automation of programs such as 5B-1, "The Prototype of the Automatic Source Code Generation Tool from UML," and "A Code Generation Method for Web Applications Based on a Tabular Form UI Model," has been researched [6][7], an automated program that can construct the screen of the Android phone from the mind map did not exist.

First, we looked at developing a tool that improves the existing software named FreeMind for a mind map [8]. However, it was very difficult to develop this tool because we did not know the program interface of FreeMind. Therefore, we decided to develop a function in GST for building the mind map to automatically generate the screen of the Android phone.

Figure 1 shows the flow of operation of the two tools, BTG and GST. The authors of the guidelines input the data with a mind map format by using GST and paper guidelines. After the guidelines and additional data are inputted to GST, the same guidelines are outputted in XML format. Then, the guidelines in XML format are read into the Android phone and the guideline content is displayed automatically on the Android phone by using the BTG. The authors of the guidelines can check the display by showing the content of the guidelines on the Android phone before shipping the BTG to the workers. If there is an error in the data, the authors of the guidelines can correct it before the workers use the guideline tool. Moreover, it is also easy for

the authors to change the content if the workers have a problem after the authors have shipped the BTG and the data.

Next, we describe the two tools in more detail. The development environment for the two tools is shown in Tables 1 and 2.

Fig. 1: Flow of operation of the two tools, BTG and GST

Table 1: Development environment of the GST

Language	C#
SDK	Net Framework 3.5 SP1
Development OS	Windows Vista Business

Table 2: Development environment of the BTG

Language	Java 1, 6, 0_21
SDK	Android SDK 1, 6
Development OS	Windows Vista Business

3.2. BTG to Display the Content of the Guidelines on the Android Phone

To enable workers to perform suitable activities without viewing evidence preservation guidelines in advance, we investigated the screen of the Android phone to make it easier to work with. As a result, we know that the objectives can be achieved by repeatedly using the following three screens (see Fig. 2).

- Menu screen

This screen is used when the application starts.

- Branching screen

This screen is used to select the answer from questions by using radio buttons.

- Conditions screen

This screen is used for selecting all answers to the questions by using checkboxes.

In addition, when workers are performing the activities on evidence preservation, The forensic authorities would like to have the evidence that the workers did not work illegally. The Android phone already has the following suitable functions.

- Camera Features

The camera in the Android phone can be used to take pictures for the preservation of evidence while working on the preservation of the evidence guidelines. The photo data can be the evidence confirming that no illegal activities took place.

- GPS Features

The GPS in the Android phone can be used to confirm the place of the work. The data can be the evidence where the work was done.

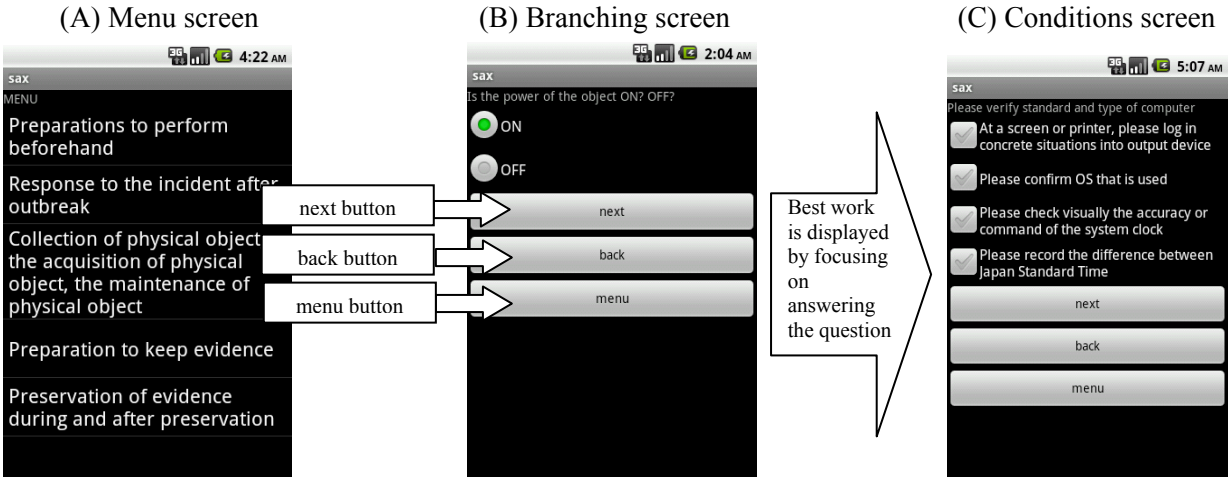

Fig. 2: Android screen displaying the content of the guidelines

3.3. GST (Guideline Support Tool)

This tool has the function to generate the guidelines in XML format from a mind map for displaying the guidelines on screens of the Android phone. To achieve this objective, the three screens shown in Fig. 2 must be prepared in the output data of the GST.

Because a conventional mind map cannot input the information that represents these screens in the Android phone, we developed a revised mind map to automatically display these screens.

The main screen of the GST procedure is shown in Fig. 3. The meanings of the buttons representing the functions are explained in Table 3. The output data of the GST is made according to the procedure displayed in Fig. 3.

First, if the “Making a project” button is pressed, new guideline generation is started after constructing the menu. If the “Reading of guideline” button is pressed, the guideline being made appears in the shape of a tree view, as shown in Fig. 4. Then, the tree view is generated or modified by using the icons having the functions shown in Table 4. Here, we realize the functions of the mind map, such as making the icon, deleting the node, editing the node, or replacing the node by another node. In addition, the answer to the question can be entered only when the answer icon is selected. In addition, the icon of the selected screen information is displayed at the left of the answer (e.g., the icon of the check button is displayed when a condition screen is chosen). In this way, it becomes easier to understand the support by the visual display.

When this tree view is completed, the output of the GST can be used to display the screens on an Android phone by using the BTG.

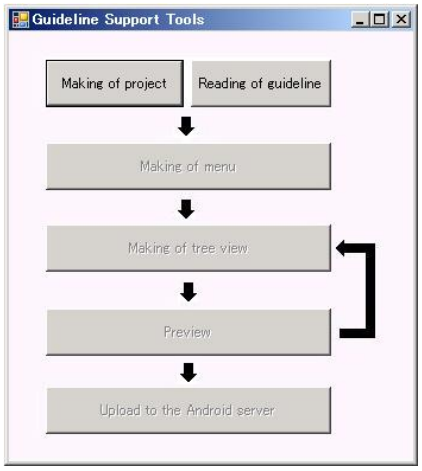

Fig. 3: Guideline support tool screen

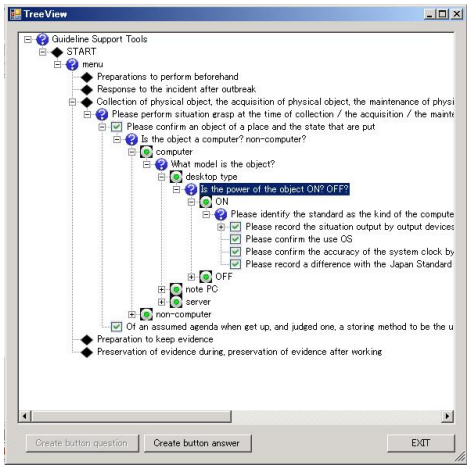

Fig. 4: Tree view screen

Table 3: Attributes of the GST tags

Button representing a function	Purpose
Making of project	The name of the project's guidelines, which specify the location, is entered.
Reading of guideline	It is possible to read when there is a project made with the guideline making support tool beforehand.
Making of menu	The content of the menu of the guideline is input.
Making of tree view	Details of the guideline are made with the icons shown in Fig. 4.
Preview	The demonstration screen, where it is easy for the made guideline to be displayed on the Android screen (Under implementation).
Upload to the Android server	The guideline is improved in the Android Store (Under implementation).

Table 4: Function icons for the tree view

Icon type	Function
	Represents the question sentence.
	Represents the divergence of the answer.
	Represents the condition of the answer.
	Represents the menu of the answer.

Figure 5 shows the output XML format guidelines from the GST. Table 5 describes the attributes of the tags in Figure 5.

```
<?xml version="1．0" encoding="UTF-8"?>

<root no="1" key=" Is the power of the object ON? OFF?" type="question" pattern="radiobutton" nextno="0" />
  <item no="1" key="ON" type="answer" pattern="radiobutton" nextno="3">
    <item no="2" key=" Please have the following tasks" type="question" pattern="radiobutton" nextno="100">
      <item no="2" key=" Do not turn off the power supply. " type="answer" pattern="radiobutton " nextno="100" />

                                                    .
                                                    .
                                                    .
    </item>
  </item>
  <item no="1" key="OFF" type="answer" pattern="radiobutton" nextno="3">
    <item no="3" key=" Please have the following tasks" type="question" pattern="radiobutton" nextno="100">
      <item no="3" key=" A surrounding person is called. " type="answer" pattern="checkbox" nextno="100" />
    </item>
  </item>
</root>
```

Fig. 5: XML code

Table 5: Attributes of the XML tags

Attribute	Explanation
no	The screen number is shown.
key	Representing a character on the screen.
type	Either the question sentence or the answer is shown.
pattern	Either the radio button or checkbox or menubutton is shown.
nextno	The transition number is shown.

3.4. Procedure in BTG after Reading the Guidelines in XML Form

Here we describe how to build a screen of the Android after reading the guidelines derived from the XML output of the GST. The explanation for constructing the screen of the Android is presented in Fig. 6. One icon represents one tag. A "no" tag represents the number of the screen. The "key" of the "type" element is a "question" displayed in the question field. The "key" of the "type" element is the "answer" displayed in the answer field. When one presses the “Next” button to load the selected “next no” answer, the screen displays the screen numbers.

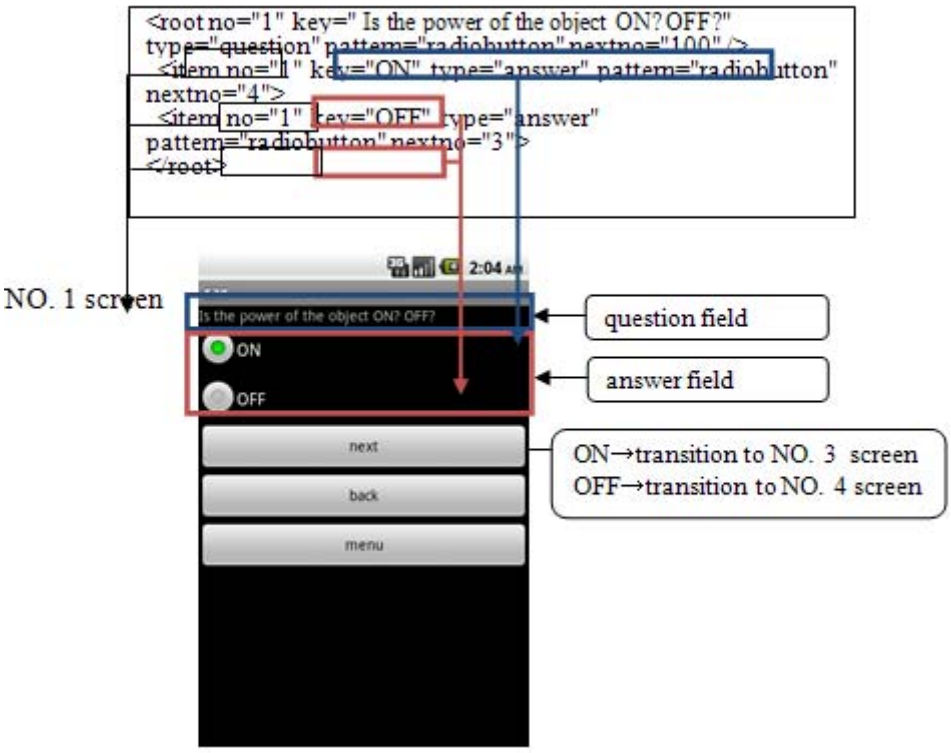

Fig. 6: Flow of Android screen construction from the XML form guideline

4. Conclusions

In this paper, to solve the problems of the preservation of forensic evidence, as set forth by the Committee on Guidelines for Digital Forensic Institute, we developed a system consisting of the GST _in PCs for the authors of guidelines and the BTG for workers using Android phones to produce the guidelines easily.

In the near future, we would like to evaluate the usefulness of the two tools by applying them to actual problems.

5. References

[1] Ryoichi Sasaki, “Trend on Digital Forensics(Tutorial)”, J. IEICE Vol.91, No.8, pp.744-745

[2] Digital Forensics Research Council Committee("Technology" Working Group Chair) Tetsutaro Uehara: GeneralGuidelines of the preservation of evidence, published April 05, 2010, http://www.digitalforensic.jp/eximgs/100405gijutsu.pdf

[3] Taro Inaba, Shinya Tahara, Nobutaka Kawaguchi, Hidekazu Shiozawa, Hiroshi Shigeno, Kenichi Okada, “Worm Path Identification for Digital Forensics”, J. IPS. 50(3), 1002-1011, 2009-03-15

[4] Nakayama Yuki, Inaba Taro, Shibaguchi Seiji, Okada Ken-ichi, “Visualization of Transmission Route of Confidential Data”, IPSJ SIG Notes, 2009(3), 31-36, 2009-01-15

[5] Digital Forensics Investigation, Sample Mind Map, http://www.ji2.co.jp/forensics/map/index.html

[6] Kawamura Yoshitsugu, Tsuchiya Takashi, Asami Katsushi, “5B-1 The Prototype of the Automatic Source Code Generation Tool from UML”, Proc. 71th Annual Convention IPS Japan (1), pp.279-280, (2009)

[7] Watanabe Keisuke, Amanuma Toshiyuki, Asami Katsushi, Imamura Makoto, Okada Yasuhiro, “D-13-1 A Code Generation Method for Web Applications Based on a Tabular Form UI Model”, Proc. IEICE Gen. Conf. 2008_Information/Systems(2), pp.265, (2008).

[8] Club use FreeMind - free mind mappingsoftware, http://www.freemind-club.com/