[Practical Paper] An evidence preservation method for a portable terminal by using data prioritization and signature history intersection

Takashi Mishina*, Yoh Shiraishi**, and Osamu Takahashi**

*Graduate School of Systems Information Science, Future University Hakodate, Japan
**School of Systems Information Science, Future University Hakodate, Japan
{siraisi, osamu}@fun.ac.jp

Abstract – A portable terminal currently contains not only a lot of personal information such as addresses, telephone numbers, e-mail addresses but also personal behavior information such as telephone call history, operation log, location information. As corporate use of portable terminals increases, it will become necessary to prove the cause of computer security incidents to decrease information leaks due to human factors.

In order to reduce such computer security incidents and prove a user's behavior, we apply digital forensics to a portable terminal. Digital forensics is a technique that collects and preserves evidences to prove information security incidents. When applying the technique to a portable terminal, we need consider the following problems: unexpected data loss on the terminal, the few calculation resources of CPU and memory, poor reliability of collected and preserved evidences.

This paper proposes a practical method of evidence preservation for a portable terminal to solve the above problems. Our method periodically collects various kinds of data on the terminal and preserves them as evidences on a server through a network. For load reduction on the terminal, data on the terminal are prioritized and collected at the frequency based on the priority level. To prevent the signature from the counterfeit and improve the evidence reliability, we adopted the signature history intersection and hysteresis signature.

Keywords: Evidence preservation, portable terminals, digital forensics, security, signature history intersection.

1 INTRODUCTION

Portable terminals are important devices that many people use for various purposes from personal use to corporate use, such as voice communication, sharing information in data communications, and internal and external access to corporate intranet systems. Moreover, portable terminals use ad hoc networks and exchange information, for example, during natural disasters. Further developments in portable terminal technology will produce more applications.

In these situations, important personal information is used such as addresses, telephone numbers, e-mail addresses, telephone call history, operation logs, file information, etc. When personal information is used for corporate use, information security measures are needed. Current information security measures have been chiefly designed to prevent invasion and operation from outside the network. However, information leaking from the inside to the outside is also a problem. Ninety percent or more of the information security breaches in which information leaks from the inside to the outside is attributed to three human factors: "ignorance", meaning information is mistakenly leaked out; "fault", meaning the terminal is operated incorrectly, lost, or stolen; and "intention", meaning information is intentionally sold illegally [1].

There are two methods for decreasing the breaches caused by these human factors. One is continuously educating the person. The other is giving the portable terminal physical measures and covering the person's mistake. The problem with education is it is expensive and takes time to see effects. Therefore, we apply digital forensics to the portable terminal, and focus on methods for decreasing the negative effects of the human factors.

Collecting periodically evidences in a portable terminal and preserving these evidences are required while a user operates the terminal as usual (namely, without stopping the system) in order to prove a user's behavior at occurring information security incidents. Also, ensuring reliability of the preserved evidences is required. It is desirable to collect and preserve as much information as possible such as telephone call history, transmitted and received information via mail, operation logs, setting files. Recently, portable terminals as smartphones are equipped with many sensors such as GPS, IC tag. By using these sensors, it is being able to collect information about a user's behavior such as movement, entering / leaving a room, electronic payment at a store. These information can be evidences to prove a user's behavior: where a user is, what a user is doing at the time.

Digital forensics [2] is a set of techniques in which evidence is collected, stored, and analyzed to prove information security incidents such as an illegal invasion, leak of information, etc. However, there are problems with digital forensics. Sometimes if information is not collected, its performance decreases and stops the system, detection is delayed, and evidence can be destroyed during an investigation [3]. In order to deal with these problems, live forensics that periodically collects evidences without stopping the system has been proposed [3][4]. This characteristic of live forensics is required for collecting evidences in a portable terminal. However, the existing methods for live forensics focus on data on personal computers with rich computation resources, and it is difficult to apply these methods to portable terminals with poor computation resources such as CPU and memory.

In addition to these problems, there are some specific problems when digital forensics is applied to portable terminals: illegal access by enhancement of communication functions, data memory composed of flash memory, and unreliable evidence [2]. Volatile data on flash memory in a

portable terminal are lost at the power off. Consequently, important evidences on the flash memory will be lost by the sudden system shutdown and battery off. There is a possibility that hardware reset by fault and malicious intention eliminate all of the evidences from the system. Preserving evidences in a portable terminal has a significant risk. Assuming illegal access from outside of the terminal, it is difficult to secure reliable evidences using only the terminal.

Therefore, our research aims to prove information security incidents caused by the human factor with a portable terminal and to prove how the terminal (namely, the user) behaves. In this paper, we apply digital forensics to a portable terminal and propose a method that periodically collects much information in a portable terminal as evidences and preserve them. The proposed method solves the problems when applying digital forensics to portable terminals and has the following characteristics.

a) Our method preserves evidences collected from a portable terminal on a remote server via a network in order to deal with vulnerability of preserving these evidences in only the portable terminal.
b) It collects evidences in a portable terminal at the different frequency according to characteristics of these evidences (volatility of data, overhead at collecting data) in order to consider limited computation resources of the terminal. We prioritize the evidence data and decide the collecting frequency based on the priority level.
c) It intersects signature histories between a portable terminal and a server in order to improve the reliability of the preserved evidences. In addition, we use the hysteresis signature technique together in order to prevent the signature from counterfeiting.

2 RELATED WORK

In this section, we clarify the position of the proposed method in the field of digital forensics, details details an existing digital forensic method for portable terminals (mobile forensics) and signature techniques to secure reliable evidence (the hysteresis signature and the signature history intersection).

2.1 Digital forensics

In digital forensics intended for the computer, usually data is maintained by the following process: (1) to detect information security incidents, (2) to judge whether evidence data disappear by turning off the power supply, (3) to turn off the power, and (4) to maintain data from the outside with some special equipment. The data disappears when the computer is switched off, but it is a possibility to add some changes to the data by collection activity.

Recently, there is other approach that tries to collect evidence data without turning off the power (namely, stopping the computer). This approach is called “live forensics” [3][4]. Since a user is always carrying a portable terminal, the characteristics of live forensics is desirable use for collecting evidence data from the terminal. However, it is difficult to apply these methods to data on portable terminals with limited computation sources. The existing methods for live forensics deal with data on computers with rich computation resources. In the case where these methods apply to portable terminals, there is a possibility that data collection activities increase the load of the computer and change the state of the system.

“Network forensics” [2] is a technique that collects and preserve data flowed on a network as evidences. Many tools for network forensics have been developed. These tools monitors network nodes such as terminals, servers and relay nodes, and collects evidence data on a network. However, this study focus on not only information flowed on a network such as call history and receiving/transmitting information, but also information recorded inside a portable terminal such as operation logs and application data. Network forensics is not enough for evidence preservation on a portable terminal.

2.2 Mobile forensics

Mobile forensics is a set of techniques that collect information inside portable terminals such as PDA and memory card as evidences in order to prove illegal use of a user with a portable terminal and prove the user’s behavior.

2.2.1 Forensics method using portable terminal memory

Willassen suggests two methods of investigating information that has been deleted from the memory of a portable terminal [5]. One of his methods uses seven pieces of information as evidence.

- Images
- Sounds
- Multimedia messages
- WAP / web browser history
- Email
- Calendar items
- Contacts

In the first method, it is connected to the on-board flash memory tip directly and reads the content of the memory. The second method uses the boundary scanning test, which is an inspection method that uses an IC tip to read the contents of the device’s memory. Both methods need a physical connection to the portable terminal, but the correct information cannot be found with a portable terminal alone.

2.2.2 Digital forensic method using a portable terminal itself

Kunii proposed a system for digital forensics and files management in a small-scale computing environment [6]. In this method, the PC files are distributing preserved. Each user proves the legitimacy of each other's file update histories and realizes digital forensics. The portable terminals are used to generate signatures in this method. However, because information in the portable terminal is not collected, it is difficult to determine what has happened using the portable terminal.

2.2.3 Device seizure

Device seizure [7] is a forensic tool for cell phones, PDAs, and GPS devices. The features all preserve the files of the original data and can run the processes of collection, preservation, and analysis independently. PDA seizure requires connection with a special device when collecting various data.

2.2.4 SIMIS

SIMIS [8] is a forensic tool for SIM cards. The features of SIMIS correspond to SIM card data collection and analysis, composed of a control card, a data preservation card, analysis application, and card reader. The features of each process ran independently. SIMIS uses cable when collecting physical copy of SIM card. SIMIS requires connection with a special device when collecting data.

2.3 Improving reliability of evidences

2.3.1 Signature history intersection

The signature history intersection [9] is a chain method between one's signature history and others' signature histories used as the signature record. As a result, it is thought that the counterfeit becomes difficult as histories become longer because it needs the falsification of others' signature histories when a person illegally forges the signature (Fig. 1).

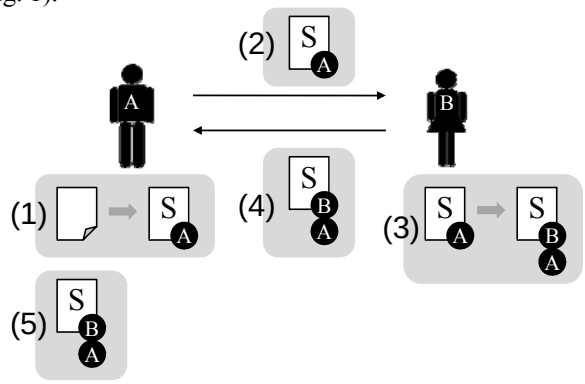

Figure 1: Signature history intercrossing

2.3.2 Hysteresis signature

The hysteresis signature [4][9] is one of the measures technologies to reduce damage because of the leakage and the presumption of the signature generation key that becomes a problem when a long term of the electronic filing document is operated a minimum. When the electronic filing document is registered, signature information is left for the history in this technology. When the electronic filing document is signed, signature information left for the history is taken and a new signature is generated. Therefore, a time series chain architecture arises between electronic documents. Concretely, the signature generation processing of the past is done by uniting the hash values of the electronic filing document to be signed and the signature record immediately before, and using own private key and the message with the hysteresis signature is generated. Moreover, signature information is left for the history at the same time (Fig. 2).

A part of the signature history is safely kept by the tamper resistant module. As a result, even if a past signature is forged, this can be detected by confirming whether it corresponds to the history.

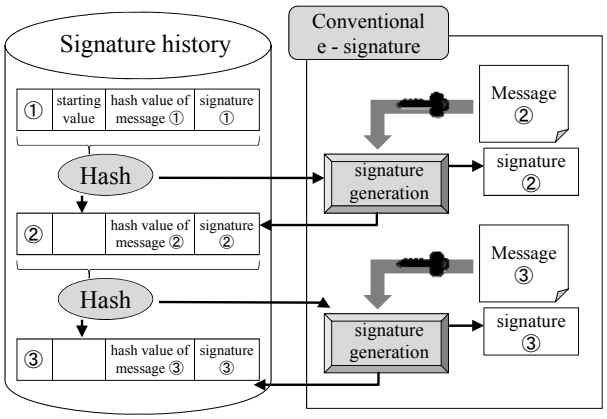

Figure 2: Hysteresis signature scheme

When the hysteresis signature is inspected, usual signature verification by the public key is done to the message with the hysteresis signature. Moreover, it can be confirmed whether there is information on a past signature in the message with the hysteresis signature as a correspondence verification of the signature generation history when inspecting it, and confirm the chain of the signature record. Therefore, it is necessary to reflect the time series chain architecture between electronic documents that not only forge the signature by counterfeiting the document to counterfeit the document with an illegal person and the signature and using electronic document manufacturer's private key but also reflect a past signature generation history and to counterfeit. It is thought that the forgery of the signature is difficult for using the hysteresis signature from the above-mentioned.

3 PROPOSED METHOD

This section describes requirements when digital forensics is applied to the portable terminal, priority level and collection frequency of information, and the flow of the proposed method.

3.1 Requirements

As described in Section 1, there are various problems when applying digital forensics to a portable terminal. We decide the requirements of an evidence preservation method for a portable terminal based on the above discussions.

a) To deal with the risk of unexpected loss of evidences on a portable terminal.

A portable terminal uses the flash memory for the data carrier and can delete all information by hardware reset. Signs of the relevant information leakage possibly cannot be acquired when evidence is maintained in the terminal. When connecting a portable terminal with a special device and collecting evidences by the device, it is difficult to collect these evidences anytime and anywhere because a user is carrying the terminal basically. Consequently, to deal with the loss of the evidences, collecting periodically data and preserving the collected data on an appropriate site as evidences are required.

b) To collect and preserve evidence data with consideration of the limitation of computation resources on a portable terminal.

When connecting the portable terminal to the special equipment from the outside and collecting evidence data, it is necessary to stop the system. Such method is unsuitable for the portable terminal that a user carries and operates anytime and anywhere. When a lot of calculation resources are needed for the portable terminal in such method of frequently acquiring the bit stream image, the performance of the system worsens. The decrease in performance and the stop of the system make it impossible to contact in the emergency. Consequently, data collection and evidence preservation without decreasing the performance and stopping the system are required.

c) To secure reliability of evidences collected from a portable terminal.

When collecting and preserving evidence only with the portable terminal and putting the e-signature on the evidence by itself, the private key leaks become possible to counterfeit of the e-signature. Moreover, evidence may be falsified by a malicious operation because the telecommunication facility of the portable terminal has been enhanced. Therefore, evidence must later be verified to make sure it is not falsified.

To satisfy these requirements, we adopt the following approach.

A) Our method collects data periodically from a portable terminal and preserves these data as evidences on a server via a network.

B) It prioritizes data in the portable terminal and collects at the frequency based on the priority level in order to reduce the load of the terminal.

C) It prevents the e-signature from the counterfeit by intersecting the signature histories between the portable terminal and the remote server, and secures the reliability of the evidences.

3.2 Priority level and collection frequency

3.2.1 Priority level of information

The data of PC and the portable terminal exists in volatility and nonvolatile states. Nonvolatile data is the data (like file system stored in the hard disk drive and the flash memory) that continues after the computer is switched off. Volatility data indicates the disappearing data (like the present network connection of the system) when turning the computer off. Table 1 shows the list and the priority level of volatility and nonvolatile data of the portable terminal.

Table 1 refers to the priority levels when data was collected that are generally recommended [10][11].

Priority levels are decided by considering the burden given to the portable terminal. "Content of memory" should acquire the memory image of the bit stream. Therefore, “content of memory” is the lowest priority level in volatility data.

About priority level of the nonvolatile data, these information that call record, SMS/MMS information, etc. are unique information of portable terminal. Therefore, we thought that these information are needed in a proving situation of human factor incidents of using portable terminal. The bit stream image can generate a copy including the space domains of the original medium. However, an execution time longer and the burden on the terminal more than that for a logical backup that copies a file simply are needed. Because as many as a seventh to an eighth of the nonvolatile data are needed to acquire the bit stream image, the priority level is low.

Table 1: Volatile data and nonvolatile data

		Volatile data	Nonvolatile data
Priority	1	Network connection	Call record
	2	Login session	SMS / MMS record
	3	Running processes	Contact information
	4	Opened files	Calendar information
	5	Network composition	Config file
	6	Time of OS	Log file
	7	Content of memory	Data file
	8		Application file

3.2.2 Change in collection frequency

With the priority levels that we showed in Section 3.2.1, we collect and maintain evidence in three phases. Table 2 lists the collection range and frequency of the evidence.

The high collection frequency acquires logical backup from volatility data priority level 1 to 6. The medium collection frequency acquires the image of the bit stream of RAM and logical backup from nonvolatile data 1 to 2. Finally, the low collection frequency acquires the image of the bit stream of ROM. By changing the collection frequency and range of information gathering, it is possible to prevent the system degrading the performance and being stopped by lowering the burden on the terminal. In addition, there is the difference in collection frequency, but the loss of evidence can be prevented to collect all information. As a result, we can solve problems (a) and (b) in Section 3.1.

Table 2: Collection frequency and collection range

Frequency	Range
High	Volatile data: priority 1 ~ 6
Medium	Volatile data: priority 7 Nonvolatile data: priority 1 ~ 6
Low	Nonvolatile data: priority 7 ~ 8

3.3 Algorithm of proposed method

The proposal method is composed of the portable terminal and the server. The portable terminal gathers and transmits evidence. The server secures maintenance and

reliability of the evidence that has been sent. The server can be trusted enough like providers of digital certification services, and the access in the server must be severely limited. Figure 3 shows the flow of the proposal method.

3.3.1 Behavior of portable terminal

The portable terminal is processed as follows.

・Regular acquisition of evidence

・Generation of hysteresis signature

・Encryption and transmission of evidence and hysteresis signature

Evidence is regularly acquired by using the collection frequency and the range of the collection of evidence listed in Table 2. To minimize effects on the system, the program that gathers evidence is executed in the conserved region near a tamper resistant SD memory card. Moreover, to prove the completeness of evidence, the hash values with former data are compared. Collected evidence is stored in the SD memory card.

Next, the hysteresis signature is generated by using acquired evidence and signature history. Afterwards, evidence and the hysteresis signature are transmitted to the server, after which evidence is deleted and the hysteresis signature is preserved as the latest signature history. Information leaks are prevented by deleting evidence. When the hysteresis signature is received from the server, it is preserved as the latest signature history. The hysteresis signature is generated and the signature history preserved in separate processes in each range of the collection.

Evidence and the hysteresis signature are both transmitted an odd number of times, but only evidence is transmitted an even number times. By right, two or more terminals acquire data respectively, and the hysteresis signature is signed in the chain. However, in this process, only the portable terminal acquires data and a chain signature with the server is enabled. The reliable evidence can be secured by this process, and the problems described in Section 3.1 can be solved.

3.3.2 Behavior of server

The server is processed as follows.

・Reception of evidence and hysteresis signature sent from portable terminal

・Generation and transmission of hysteresis signature

All evidence and the hysteresis signatures sent from the portable terminal are preserved on the server side. The hysteresis signature is generated, and signature history preserved in separate processes in each range of the collection as well as the portable terminal side. The hysteresis signature is not generated and transmitted an odd number of times but an even number times (Fig. 3). Because evidence is preserved only on the server side, evidence can be prevented from being falsified.

4 EVALUATION AND DISCUSSIONS

This section shows the effects of the human factor with which the proposed method can deal and the results of the qualitative evaluation.

4.1 Incidents that can be dealt with

The biggest cause of information leaks is "operational errors", in which information is leaked through e-mails sent to the wrong recipient. The second biggest cause is "management mistakes", in which important information is mistakenly leaked out with other information. Other causes of leaks are losing or leaving behind memory devices that contain important information, theft, illegal removal of information, configuration errors, etc. Using the portable terminal with the proposed method enables these human factors to be proved.

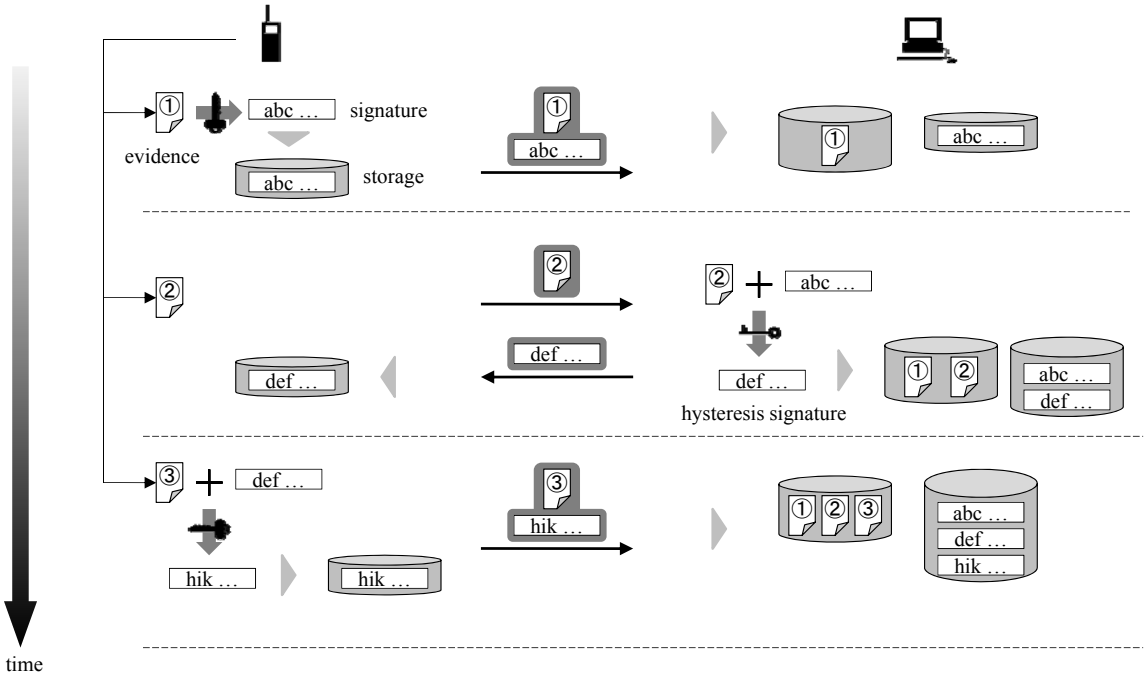

Figure 3: Flow of the proposed method

(1) Ignorance

This includes management mistakes and configuration errors. When important information is thrown away by mistake, proposed method can prove when, how and what information was thrown away. At that time, proposed method uses running processes, time of OS, and data files. When the information leaks due to a setting mistake in the application, the cause can be proven. At that time, configuration files and application file are used.

(2) Fault

This includes operational errors, theft, loss, or leaving the device unattended. Proposed method can prove what e-mail has been sent by mistake due to operational error by the portable terminal. At that time, proposed method uses the network connection, network composition, and log file. This can determine whether the portable terminal was being operated while it was lost or stolen. At that time, xxx checks the login session, running processes, and opened files. The proposed method should be able to determine whether someone had the portable terminal.

(3) Intention

This includes illegally removing information. The proposed method can prove what information has been illegally removed by using with the address and the telephone number, etc. At that time, proposed method uses data files and the content of the device memory.

Much volatile data with high collection frequency is requested in typical information leaks. It is thought that problems can be dealt with because a lot of volatile and nonvolatile data are collected in the proposed method even when incidents other than those above occur. When the cause is proven, proof that keeps the temporal order is possible because data and the hysteresis signature of information are acquired regularly.

4.2 Qualitative evaluation

The case where existing digital forensics of the computer is applied to the portable terminal is defined as "non-apply" and is carried out as follows. The portable terminal is connected to a PC, and an image of the RAM bit stream is acquired. Afterwards, the ROM data is maintained as a bit stream image while the portable terminal system is stopped. Table 3 shows the results of the qualitative evaluation by comparing the "non-apply" and the proposed method.

Table 3: Qualitative evaluation results
(O: good , Δ: poor , X: no good)

	Non-apply	Proposed method
Mistake acquisition	O	Δ
Performance degradation	X	O
Reliability	O	O

The problems enumerated in Section 3.1 were used to evaluate the method.

(1) Mistake acquisition of information

Non-apply collects and maintains the ROM and RAM data as a bit stream image. Therefore, non-apply can reduce miss acquisition of information by collecting and storing it as soon as security incidents happen.

The proposed method acquires images of the ROM and RAM bit stream. However, the information acquired is frequently a physical data copy of volatile data. Therefore, nonvolatile data may be missed in some cases.

(2) Degradation of the system

In non-apply, there is no communication in an emergency because the portable terminal must be stopped.

In the proposed method, the collection frequency and the range of the collection are changed in accordance with the priority level of information. Therefore, the burden on the portable terminal is small, so it is never stopped.

(3) Reliability of the evidence

To connect with a trustworthy PC and to gather evidence in non-apply, the reliability of the evidence is secured enough.

In the proposed method, collected evidence is preserved in the portable terminal once. However, it is thought that the reliability of evidence is secure enough so that hysteresis may be signed between the server and the portable terminal, and the servers preserve evidence for a long time.

This qualitative evaluation showed that, when non-applying, the proposed method was inferior at preventing information from being deleted. However, it prevented degradation of system performance, which is the most important thing in the portable terminal.

4.3 Quantitative evaluation

4.3.1 Experiment environment

We implemented the proposed method as an application and quantitatively evaluated the proposed method for three processes.

- Regular acquisition of evidence
- Generation of hysteresis signature
- Encryption and transmission of evidence and hysteresis signature

The experimental environment is as follows (Table 4).

Table 4: Experimental objects

OS	Android 1.6
Terminal	HT-03 A [12] CPU : 528 MHz Storage : 512 MB Memory (RAM) : 192 MB
Network	IEEE 802.11 g
Symmetric-key cryptography	AES 128-bit key
Public key cryptography	DSA 1024-bit key
Target data (from Table 2)	High-frequency data Low-frequency data

Experimental items are as follows.

(1) CPU load

The CPU load on to the terminal in each of the three processes for the proposed method.

(2) Memory usage

Memory usage shows the memory area used in each of the three processes for the proposed method.

(3) Runtime

During the acquisition process, the runtime shows the time until the application finished the evidence acquisition starting.

The measurement method is as follows.

・One of the three processes, acquisition, signing, or transmission from the portable terminal, is run.

・The running load is measured using the vmstat command.

・The mean is calculated using five measurements

As a prerequisite for evaluation, I finished all applications except for the application of the proposed method, and I evaluated the proposed method at a stationary state of about 0–3% CPU load for the system.

4.3.2 Experimental result

(1) High-frequency collection

Table 5 shows the result of the quantitative evaluation using high-frequency collection.

The CPU load when the evidence was acquired was low, and the runtime was short. The CPU load when evidence was signed was highest, and the runtime was the shortest. The CPU load when the evidence was encrypted and transferred was high, and the runtime was longest. Therefore, this process puts a heavy workload on the portable terminal. I thought the difference between the signature and encryption was due to the difference of the processing data volume. In the signature process, the proposed method sign for the hash value from original data. However, in the process of encryption, the proposed method encrypts the original data. The data volume of the original data is larger than the hash value. I found that the memory usage was always low.

Table 5: Result of the high-frequency collection

	CPU (%)	Memory (MB)	Runtime (s)
Acquisition	16.7	0.09	2.8
Signature	98	0	0.03
Transmission	71.4	0.96	9.3
Average	58.83	0.76	(Total time) 12.13

(2) Low-frequency collection

Table 6 shows the results of quantitative evaluation by low frequency.

This result shows the same tendency as the high-frequency, because the only difference between low- and high-frequency is the volume of data. However, the runtime when the evidence is encrypted and transferred is unacceptably long. This is because the proposed method encrypts and transfers the original data without dividing it.

Table 6: Results of the low-frequency collection

	CPU (%)	Memory (MB)	Runtime (s)
Acquisition	55.57	1.13	70.20
Signature	97.60	0.00	17.45
Transmission	63.15	0.11	2217.24
Average	63.19	0.14	(Total time) 2304.89

4.4 Summary of evaluation

In the quantitative evaluation, I measured the load of the proposed method for high-frequency data and low-frequency data. The portable terminal had a workload from high-frequency data of about 12 seconds and about 58% load of the CPU. The portable terminal had a workload from the low-frequency data of about 38 minutes and about 63% load of the CPU. This suggests that the proposed method can acquire volatile data without requiring the system to stop. The proposed method could not acquire, sign, encrypt and transfer nonvolatile data as a whole.

Therefore, for portable terminals, the proposed method should acquire evidence at fixed intervals, and the proposed method should sign, encrypt, and transfer at a little-used time.

5 CONCLUSION

A technique to preserve evidence was proposed to change the collection frequency and range by using the priority level of information when using digital forensics for portable terminals. Evidence that corresponds to many information leaks can be gathered by frequently collecting important volatility data and reducing the burden on the portable terminal. Nonvolatile data is collected at low frequency. Therefore, this data can correspond to the data file and the application file that are requested as proof of an information leak. The signature using the portable terminal can be verified as evidence by using the hysteresis signature. Therefore, reliable evidence can be securely maintained. Quantitative evaluation demonstrated that the proposed method was useful.

For future work, it is necessary to improve acquisition, signature, encryption, and transmission. The proposed method must process the data in parts. Moreover, it is necessary to determine the optimum evidence collection frequency while minimizing the load on the system.

REFERENCES

[1] H. Ohtani (Working Group Leader), Information Security Incident Survey Report, NPO Japan Network Security Association Security Incident Investigation Working Group (2008).

[2] S. Tsujii (editorial supervisor), Digital Forensics Dictionary, Digital Forensics Society (2006).

[3] T. Ochi, T. Kojima, M. Togawa, and Y. Itakura, “The Proposal of Incident Detection Method using the Hot Digital Forensic,” IPSJ SIG Notes 2008, pp. 267–272, Information Processing Society of Japan (2008).

[4] M. Shinoda, Y. Ueda, and R. Sasaki, “Proposal and Evaluation of Hysteresis Signature System with Paper

Document," Proc. Technical Report of IEICE. ISEC, Vol. 103, pp. 77–82 (2003).
[5] S. Willassen, "Forensic Analysis of Mobile Phone Internal Memory," Proc. International Federation for Information Processing (IFIP), Vol. 104, pp. 191–204 (2005).
[6] Y. Kunii and R. Uda, "A Proposal of A Distributed File Backup System for Digital Forensics Using Cellular Phone," Proc. Multimedia, Distributed, Cooperative, and Mobile Symposium (DICOMO 2009), pp.671–678 (2009).
[7] Paraben Corporation, Device Seizure http://www.paraben.com/device-seizure.html
[8] 3g Forensics Smart Forensic Solutions, SIMIS http://www.crownhillmobile.com/simis.htm
[9] S. Susaki and T. Matsumoto, "Alibi Establishment for Electronic Signatures," IPSJ Journal, Vol. 43, No. 8, pp. 2381–2394 (2002).
[10] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," Proc. NIST Special Publication, pp. 800–886 (2006).
[11] D. Brezinski and T. Killalea, "Guidelines for Evidence Collection and Archiving," RFC3227 (Best Current Practice) (2002).
[12] htc, HT-03A,http://www.htc.com/jp/product/ht03a/overview.html.

(Received July 6, 2010)
(Revised May 14, 2012)

Takashi Mishina received his B.E. and M.E. degrees in information science from Future University Hakodate, Japan in 2009 and 2011. His research interests include mobile computing and information security. He currently works in NTT East Corporation.

Yoh Shiraishi received doctor's degree from Keio University in 2004. He is currently an associate professor at the Department of Media Architecture, School of Systems Information Science, Future University Hakodate Japan. His research interests include database, mobile sensing and ubiquitous computing. He is a member of IPSJ, IEICE, GISA and ACM.

Osamu Takahashi received master's degree from Hokkaido University in 1975. He is currently a professor at the Department of System Information Science at Future University Hakodate, Japan. His research interest includes ad-hoc network, network security, and mobile computing. He is a member of IEEE, IEICE, IPSJ.