A Memory Acquisition Method for Android Application Forensics

To cite this article: Bin Liu et al 2019 J. Phys.: Conf. Ser. 1314 012180

View the article online for updates and enhancements.
A Memory Acquisition Method for Android Application Forensics

Bin Liu¹, Ying-xian Chang², Lian-ri Cong¹, Xia Wu¹, Hua Deng³*, Yang-chun Li³, Bo-wen Xu³

¹ State Grid Shandong Electric Power Company YanTai Power Supply Company
² State Grid Shandong Electric Power Company
³ Department of Computer Science and Technology Harbin Institute of Technology

*Author to whom correspondence should be addressed; E-Mail: denghua88@163.com (Hua Deng);

Abstract. With the rapid development of social economy, the number of Android mobile devices has increased rapidly in recent years. At present, digital forensics experts mainly extract digital evidence from non-volatile physical memory and file system of mobile devices. However, non-volatile storage based method has little effect for some high secure Apps forensics, such as the encrypted data or deleted information, e.g. the private conversation records or payment records, in chat Apps or payment Apps. Accordingly, data residential in memory is an important source of evidence. On the other hand, relying solely on digital evidence in non-volatile storage is incomplete and unreliable as well. So, the demand for memory forensic on the Android platform has increased. In this paper, based on ptrace a scheme for Android memory extraction at the process level is proposed. For this scheme, a complete memory mirror of a specific process can be achieved, including memory space shared anonymously by the process and other processes, the memory space of the process, and the memory space of each thread in process. This method is of great importance to high secure Apps forensics, such as Chat Apps or Bitcoin Payment Apps.

1. Introduction
In recent years, Android mobile devices grew very quickly. At the same time, malware and spywares evolved extensively affecting the mobile landscape [1][2]. In recent years, it is of great emergency for security or forensic techniques and tools to adapt to the new situation. In Android forensics techniques, analysis is performed in system logs, network traffic, file system and memory etc [3]-[5]. However, for some high secure Applications, the security analysis and forensics for the encrypted data or deleted conversation records, e.g. the Chat Applications or Bitcoin Payment for Gaming Applications, it remains a difficulty[6]-[10]. In this case memory based analysis and forensics is a viable solution. On one hand, data residential in memory is an important source of evidence. On the other hand, relying solely on digital evidence in non-volatile storage is incomplete and unreliable as well.

In this paper, based on ptrace a scheme for Android memory extraction at the process level is proposed. For this scheme, a complete memory mirror of a specific process can be achieved, including memory space shared anonymously by the process and other processes, the memory space of the process, and the memory space of each thread in process. In this paper, the designed method for Android memory acquisition is described in detail firstly. Then, some representative android applications are
adopted and a preliminary experiment is conducted. Experimental results demonstrate the efficacy of the designed method.

2. Android Memory Acquisition Method

With rapid development of mobile technology, the number of Android devices has increased rapidly in recent years. At present, experts extract information from non-volatile physical memory or file system of mobile devices as digital evidence. However for some high security Apps, e.g. the private conversation records or payment records in chat or payment Apps, owing to the time-bombed conversation or encrypted payment, the non-volatile storage based method is of little help to digital forensics. On the other hand, relying solely on digital evidence in non-volatile storage is incomplete and unreliable as well. Accordingly, the data residential in memory is an important source of evidence in such circumstances. So, memory forensics is of great importance to high security Apps such as the Chat or Gaming Payment Apps.

In this paper, based on ptrace a method of memory extraction for a specific Android Application is proposed. In this scheme, a complete memory mirror of a specific process can be acquired, including memory space shared anonymously with other processes, the memory space of the process itself, and memory space of each thread in the target process. The memory extraction method proposed is of great importance to high secure Applications forensics, such as the time-bombed private chat information or encrypted Bitcoin Payment records.

Based on ptrace, the proposed memory acquisition process is depicted in Fig. 1, for which the MEM image of the target process is acquired basing on the MAPS file. First, the PIDs (Process ID) of the target Android Application are acquired. Then for a specific process of the Application, the PID is ptraced. Thereafter, each line in the MAPS file is traversed and the type of memory is determined thereafter.

In the case of memory shared with other process, e.g. /dev/ashmem, the memory space is located in physical memory, and the content can be acquired by invoking the ptrace function with PTRACE_PEEKDATA parameter. Otherwise, the memory space can be acquired by exploiting the PROC of Android OS. By using the read() and write() function prototype, the memory extraction is faster than that of the shared memory.

In the case of the stack space, for which memory information can not be directly dumped by using the PROC, the shell code injection approach is deployed. A shell code is specifically designed to exploit registers to access the stack space of target process. Firstly, all the register values are saved. Secondly, the SIGTRAP is signaled to temporarily freeze the thread. After that, the shell code is injected and executed to dump all the stack space using the register operations to an output file. Lastly, the contents of the registers are recovered and the target process is resumed to execute.

After the memory acquisition, a PID.mem and PID.maps are dumped respectively, which can be saved to a specific storage server for further analysis and digital forensics.
3. Evaluations
In this work, a preliminary experiment is conducted to test the designed ptrace based Android Application memory acquisition method. In this work, the following typical Android application are adopted, e.g. Tecent QQ is the representative of chat Applications with a high degree of popularity, Google calender is the most popular personal assistant abroad, whilst gmail owns the most market share of email abroad as well. The target phone is a Nexus 5x with Android 6.0.1, and the experimental results are depicted in Table I. the preliminary experiment results demonstrate the efficacy of the designed memory acquisition approach.

| Name of App | Process Name             | pid  | number of threads | Size of MEM | Size of MAPS |
|-------------|--------------------------|------|-------------------|-------------|-------------|
| Tecent QQ   | com.tencent.mobileqq     | 16883| 126               | 1.25GB      | 106.65KB    |
| Google calender | com.google.android.calendar | 18485| 68                | 1.66GB      | 63.60KB     |
| Gmail       | com.google.android.gm    | 25745| 78                | 2.30GB      | 72.35KB     |

4. Conclusions
In recent years, digital forensics from non-volatile physical memory or file system of mobile devices are a prevalent approach. However for some high security Apps, e.g. the private conversation or payment records in high security applications such as chat or gaming Apps, owing to the time-bombed conversation or encrypted payment, it is of little efficacy. On the other hand, relying solely on non-volatile storage is incomplete and unreliable. In this paper, a ptrace based memory acquisition method is designed. In which, a complete memory mirror for a specific App can be acquired, e.g. memory space shared anonymously, the space of the process, and that of each threads in the target.
process. Consequently the information residential in memory can be exploited as a vital source of evidence. This is of great importance to memory forensics for high security Apps, such as the time-bombed featured private chat or encrypted Bitcoin Payment Applications.

Acknowledgment
Thanks to the staff of HuaQiang Co and the students in HIT. This work is supported by project SGSDYT00FCJS1800719.

References
[1] Damshenas M, Dehghantanha A, Mahmoud R. A Survey on Digital Forensics Trends. Int J Cyber-Security Digit Forensics. 2014;3(4):209–34.
[2] Dehghantanha A, Franke K. Privacy-respecting digital investigation. 2014 12th Annu Conf Privacy, Secur Trust PST 2014. 2014;129–38.
[3] Open source Android Forensics app and framework. https://github.com/nowsecure/android-forensics
[4] Cruz F, Moser A, Cohen M. A scalable file based data store for forensic analysis. Digit Investig. Elsevier Ltd; 2015;12:S90–101.
[5] NIST. Have Your Computer Forensics Tools Been Tested? In: Computer Forensics Tool Testing Handbook. National Institute of Standards and Technology (NIST); 2015.
[6] Ayers R, Jansen W, Brothers S. Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1). 2014;1:85.
[7] Umale MMN, Deshmukh PAB, Tambhakhe PMD. Mobile Phone Forensics Challenges and Tools Classification : A Review. 2014;(March):622–6.
[8] YANG, S. J., CHOI, J. H., KIM, K. B., AND CHANG, T. New acquisition method based on firmware update protocols for android smartphones. Digital Investigation 14 (2015).
[9] Signal, the Snowden-Approved Crypto App, Comes to Android. http://www.wired.com/2015/11/signals-snowden-approved-phone-crypto-app-comes-to-android/, 2015.
[10] Apple vs. the FBI: Google, WhatsApp, John McAfee and more are taking sides - LA Times. http://www.latimes.com/business/technology/la-fi-tn-tech-responseapple-20160218-snap-hmlstory.html, 2016