Android Mobile Forensic Sciences Research

Jiang Du[1, a],Bin Guo[2,b]

[1]Chongqing University of Posts and Telecommunications,China

[2]Chongqing University of Posts and Telecommunications,China

[a]clouddu@126.com, [b]guobin2100@126.com

Keywords: android forensics; electronic evidence; data extraction

Abstract. According to the characteristics of electronic evidence, the storage mechanisms of Android phone and specific operational problems encountered in forensic work are summarized. This article presents a relatively standardized evidence-based policy Android phones, hoping to improve the Android mobile phone forensics operating procedures and rules for the operation to extract the maximum extent possible traces left in the phone , while reducing or avoiding contamination of the phone caused the original data when extracting data.

Background

Often you can see from the news that someone opens the link which he or she wins the lottery or something in a text message , the result is a certain amount of money on their bank card missing. If according to traditional cases to investigate, probably nothing can be done , because the offenders seem to be no contact with someone, how to find traces of criminal offenders left, how to find the criminals, how to get the evidence to convict criminals? Today, more and more diverse and innovative forms of crime, criminals let us feel they are far away from us,but we still suffer. But criminals are never far away from us, they just upgrade forms of crime, which become covert and technical,thus we find it is difficult to capture evidence at the scene. The so-called upgraded forms, namely by means of modern technology to remote crime, so as to implement Internet gambling,pyramid sale, fraud and so on. Although it is difficult to find evidence, but the old saying goes, "A wild goose leaves behind a voice." Once bad things be done, there will be evidence left behind, which we need also use modern technology to find , to recovery, to set . As traditional cases, we believe that after several years of development, it has a relatively mature forensic processes, what about new criminal cases ?

Computer forensics also has a relatively stable policy, mobile phone and computer are also electronic products, but must be treated differently. In recent years, mobile Internet has made a fast, smart phone-based, market share soar. February 4, 2015, the Supreme Court issued "on the applicable <People's Republic of China Civil Procedure Law> explained," which defined the e-mail, online chats, blog and other electronic data can be used as evidence in civil proceedings. So it is necessary to study mobile phone forensics. Due to different mobile phones currently on the market have different system architectures,such as Android, IOS, Windows phone systems,in forensic work ,they should be treated differently , the paper mainly on Android phone forensics.

Forensics Process Research

Mobile Phone Forensics must strictly follow the legal three principles: the principle of comprehensive forensics, forensics destructive principle, the principle of timely evidence. Resolve the status of your phone data carrier data extraction and content analysis of the problem, and then sort out the relevance of the case and the time course of the case related personnel.

The research of Android phone forensics strategy in China's major colleges and universities have already started and a number of forensic institutions also conduct electronic data forensic services, have to undertake all types of civil and criminal cases. The way forensic policy institutions also vary. In this paper, combined with the author's internship experience and research experience summary.

For Android phone forensics, divided into the following sections:

1. The fixed samples

For the mobile phones sent by organizations, companies or individuals , the first step is to register, rather than pre-screening. For the civil or criminal cases involving sample sent by public security and judicial organs, samples also need to check the packaging is intact and seal samples were photographed and archived. Registration includes mobile phone brands , models , the unique phone number IMEI, as well as whether the phone's battery is disassembled, the mobile phone with a SIM card or sdcard memory card , if there is power charger device, if phone is switched on, it should be promptly shut down, so the original data is not overwritten by new data, if a password is set to unlock the phone, you should promptly ask the inspection staff. The samples should be put on in special bags,which anti-static and anti-magnetic and label and storage safely. Finally, specify the purpose of identification inspection personnel.

2. Pre-flight

Understand the need of inspection staff, the first is to test the phone, because the cause of the fault if the phone can not be repaired or technical level and other reasons can not be identified, the inspection staff should be promptly informed . If you can identify by the judicial detected, it signed a letter of intent with the submission of Forensic personnel, and cover both the office Jifeng.

3. Forensic Sciences

1)prepare

To do a good job, he must first sharpen his device. Before the phone data extraction, you should be ready to prepare appropriate software and hardware devices. Hardware including mobile phone chargers of corresponding model ,which can provide a stable voltage supply to prevent the risk of the evidence in the evidence collection process was interrupted due to insufficient power supply . Hardware device also includes a mobile phone SIM card forensics of SIM Card Reader, the phone forensic data extraction and analysis platform. The software includes the DC4500 series software, Russia Oxygen Forensic and SQLite Expert View software and so on.

2)data extraction

After preparing a good job, you can extract the data, the data on the SIM card, the data on your phone and the data on your sdcard , which needs extracted separately. For the SIM card, you can use SIM Card Reader software and hardware to read the data on phone records, text messages and phone book of the SIM card inside the store, due to the limited storage capacity SIM card itself, so the extracted data is also very limited. For sdcard data extraction either as computer forensics hard drive as read-only interface to insert a card reader with FTK Image software for the above data is mirrored and then analyze the data or you can also extract the data with the phone, but the authors do not recommend doing so, because once the phone is running, some software may run in the background, writing data sdcard above, followed by the evidence in terms of data integrity, It is evidence of damage. Therefore, it is best to extract data separately. For the phone data extraction, extraction by professional forensic software, all the data can be extracted inside the phone ROM, you can also on the part of the application software and communications information extraction.

3) Data Analysis

According to the letter of intent signed by the inspection staff about the purpose , identify the targeted data and analysis to save time and labor costs.

4)Issue a report

Finally, according to the purpose of identification , the judicial testimonial legally bound,which minutely describe the tool , the use of the accreditation process, the evidence and from what was found and identified person (minimum two persons present). Chapter stamped testing center, binding.

Summary

In this paper, the technical characteristics of mobile phone forensics and specific operating procedures in practice, little perfect for Android phones evidence of specific policies and procedures are summarized in order to improve cell phone forensics, reducing the evidence is not evidence in the proper operation of the process evidence of damage caused. Because the system version of

Android phones from different companies and the depth of customization system brought about by the mobile phone version of the differentiation and brand differentiation, giving evidence brought many inconveniences. In summing up process can only be summarized based on limited models, systems and problems, we can not regulate all aspects of the proposed set of evidence strategy. In the phone data extraction process carried out through a number of root mention the right to receive, in the root process will inevitably cause a certain degree of modification ROM, not like a computer hard drive as read-only interface for data extraction.

References

[1] Nielsen B, Jiang Du, MUSLIM, Gang main translation computer forensic investigations Guide [M] Chongqing: Chongqing University Press, 2009: 4-11.

[2] Lianfu Yin computer forensics tools [J]. Computer Systems & Applications, 2005,8: 25-28.

[3] Chengya Tian. Smartphone forensic research [D]. Shandong Institute of Light Industry, 2011.

[4] Hoog, A. (2009a, March 16). Input/output error trying to dd Android/dev/block devices. viaForensics Web site. Retrieved December 21,2009,fromhttp://viaforensics.com/forum/androidforensics/inputoutput-error-trying-to-dd-android-devblock-devices/

[5] Ayers, R., Jansen, W., Moenner, L., Delaitre, A.: Cell phone forensic tools: an overview and analysis update, NIST Technical Report 7387 (Mar 2007)

[6] Liu, H., Darabi, H., Banerjee, P., Liu, J.: Survey of Wireless Indoor Positioning Techniques and Systems, IEEE Transactions on Systems, Man,and Cybernetics – Part C: Applications and Reviews, Vol. 37, No. 6 (Nov 2007)

[7] Foursquare – About, http://foursquare.com/about, (Retrieved on Feb 16, 2011)

[8] IDC worldwide quarterly mobile phone tracker, May 2013.

[9] http://developer.Android.com/tools/debugging/ddms.html [Accessed on Nov. 2012].

[10] http://www.forensicswiki.org/wiki/dd [Accessed on Oct. 2013].

[11] http://developer.android.com/tools/help/adb.html [Accessed on Nov.2012].

