Assignment No.9

Problem Statement

Install and use Android Mobile Forensics Open Source Tools.

Theory

Forensic / Forensic science is the scientific method of gathering and examining information about the past. This is especially important in law enforcement where forensics is done in relation to criminal or civil law, but forensics are also carried out in other fields, such as astronomy, archaeology, biology and geology to investigate ancient times.

Mobile Forensics is defined as "the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods."

Introduction

Android, Google's mobile device platform, is growing quickly in its share of the smart phone market share. For the period ending February 2010, Android grew 5.2% and now has a 9% share of the smart phone market. In October 2009, a report released by Gartner predicted that by 2012, Android will be the second largest smart phone provider (totaling 94.5 million units sold), second only to RIM.

And you will not only find Android in smart phones but in tablets, e-readers, net books, home appliances, and more. The first Android device was released in October 2008 and currently there are about 35 smart phones available on the market. There are also 6 tablets, 3 e-book readers, and one net book. In 2010, a large number of new devices will be released, including 20+ smart phones, 23 tablets, 2 e-books, and 4 net books. Clearly, forensic examiners need to prepare for Android devices now.

Android Overview

Android is an open source mobile device platform based on the Linux 2.6 kernel and managed by the Open Handset Alliance—a group of major mobile device, hardware, and software vendors. The open source nature of the project has not only established a new direction for the industry (forcing behemoths like Nokia/Symbian to open source their platform) but enables a developer or code savvy forensic analyst to understand the device at the most fundamental level. As the core platform is quickly maturing and is provided free of charge, carriers and hardware vendors alike can focus their efforts in customizations intended to retain their customers.

Applications for Android are developed in Java and run in a separate Dalvik virtual machine (DVM) with a unique user id and process which is a key mechanism used to enforce data security. Applications can only access the data within their DVM unless another application and the phone owner specifically allows the data to be shared.

Forensics Strategies for Android Devices

There are four primary ways to approach forensics on an Android device. They are:

- SD Card analysis
- Logical acquisition
- Physical acquisition
- Chip-off

SD Card Analysis: Nearly every Android device comes with an external SD Card for storing data. Upon receiving and securing an Android device (as you would any other mobile device), an examiner should remove the SD Card and process it in the standard way. The card is formatted with a FAT32 file system.

Logical Analysis: The logical acquisition of an Android device is the technique we recommended first. This technique involves copying a small (~25k) Android Forensics application to the device, running the application, and then removing it from the device. An application, written by viaForensics and distributed for free to law enforcement and government agencies charged with digital forensic responsibilities, currently acquires the following information:

1. Browser history
2. Call Logs
3. Contact Methods
4. External Image Media (meta data)
5. External Image Thumbnail Media (meta data)
6. External Media, Audio, and Misc. (meta data)
7. External Videos (meta data)
8. MMS
9. MMSParts (includes full images sent via MMS)
10. Organizations
11. People
12. SMS
13. List of all applications installed and version
14. Contacts Extensions
15. Contacts Groups
16. Contacts Phones
17. Contacts Settings

And new data sources are being developed weekly. The data is written to an SD Card the examiner placed into the device. The files are currently written as CSV; however we will likely change this to an XML format.

Physical Analysis: In some cases, a more significant analysis is required. This technique requires root privileges on the device and can yield a significant amount of information.

This technique will provide a forensic image of the various user data partitions. These partitions use the open source file system YAFFS2 (Yet Another Flash File System 2) and is one of the significant challenges with the Android platform.

YAFFS2 was built specifically for the growing NAND memory devices and has a number of important features which address the stringent needs of this medium. It is a log-structured file system, provides built in wear-leveling and error correction, is fast, and has a small footprint in RAM. However, since its usage was limited prior to Android, no commercial forensic product supports the file system.

***Chip-off**:* Chip-off is a technique where the NAND flash chips are physically removed from the Device and examined externally.

Design Analysis / Implementation Logic:

1) Download (.apk) one of the Android Mobile open source Forensic tool (Ex. AFLogical OSE)

2) Install .apk file on any Android based Mobile.

3) After successful installation run that tool and capture the required information (ex. Call logs, SMS, MMS etc.)

Conclusion:

Hence, we have installed and used the Android Mobile open source forensic tool.