Advanced Computer Forensics
Ruiyang Liu 85C576
Conference Paper Summary – Group #5

Paper selected: Toward a general collection methodology for Android devices
Paper author: Timothy Vidas, Chengye Zhang, Nicolas Christin
Word count: 725 words

Traditionally, mobile device forensics has been constrained by a variety of requirements particular to different manufacturers and versions of devices. Devices may differ in terms of their cables, interfaces, and physical form factors, among other characteristics. In addition, there are numerous differences in software, memory layouts, and storage mechanisms across different devices, as well as between different operating systems. Because of this, forensic data collectors are required to handle a diverse range of cable types as well as be proficient in a variety of data collection procedures. As part of their training, forensics analysts are expected to have a plethora of expertise assessing a variety of various types of material.

Android has a large market share today and is becoming a prominent operating system in many mobile devices. Because of the widespread use of Android, forensics may be performed more conveniently. With Android, the variety of digital forensics tools that are necessary is reduced to a bare minimum. Sound data collecting is made even easier with Android's enhanced audio capabilities. First and foremost, Android is based on the Linux kernel. Android applications are written in Java and interface with the well-defined APIs provided by the Android framework, which is used to create the majority of Android applications. With the Android Debug Bridge (ADB), scientists can examine debug information and do a variety of additional tasks on Android-based mobile devices. Finally, Android is an open-source project, which means that all of the code has been made publicly available and can be simply assembled.
Data preservation, atomic collection, accuracy, determinism, and usability are all goals of data collecting. Other goals include data security and privacy.
When collecting data, researchers prepare a collection recovery image that is then flashed onto the device by a research assistant. As soon as that is completed, users can reboot the device into recovery mode and connect it to a computer that is equipped with ADB. They can use the ADB to check and run apps from the recovery image, among other things. The recommended approach for collection is to track the port forward TCP ports from the device using the adb

command line interface. Researchers can move data from storage devices to the local device TCP port by launching a receiving process on the computer and waiting for the data to arrive.

Aside from that, Android devices are composed of a number of partitions that are often mapped to MTD devices. Rooting a device is not always encouraged in forensics, and in many circumstances it is not even possible. Rooting may cause elements of the user's data to be altered, as well as the Android security mode to be compromised.

In addition, the author of this paper presents various instances of specific devices to consider. The Motorola Droid includes a specific flash boot mode that allows it to boot faster. The recovery partition can be flashed more easily with the help of the Motorola RSD light program. However, a booting file in its natural format will not be accepted by this device. The HTC G1 includes a booting method known as Fastboot, which can enumerate the devices that have been attached as well as flash an image to the device that has been attached. Additionally, the HTC G1 may be used to directly boot to a kernel and ram drive when connected to a computer through USB. Samsung Captivate makes use of the company's own RFS and OneNand memory, which includes an unique flash for enhanced performance.

The paper presents an example of a general strategy for collecting digital forensics evidence from Android smartphones. By utilizing specific boot procedures that allow for the usage of custom recovery booting, data on Android devices can be captured more accurately and safely, with little chance of causing damage to the device's personal data. This article also conducts a number of experiments on a variety of devices. Also mentioned is that the software already installed in collection bootings can be readily expanded in the future, according to the creator. Apart from that, a full set of bootings supporting all Android devices will be generated and maintained, as well as thoroughly tested.