Investigating Information recovered from Re-sold Mobile Devices

Tim Storer
School Of Computing Science
University of Glasgow
tws@dcs.gla.ac.uk

Wm. Bradley Glisson
HATI Institute
University of Glasgow
b.glisson@hatii.arts.gla.ac.uk

George Grispos
HATI Institute
University of Glasgow
0906129G@student.gla.ac.uk

ABSTRACT

The data storage capacity mobile digital devices is continually increasing, with a corresponding potential for such devices to retain sensitive personal and corporate information. Simultaneously, the increasing complexity of mobile devices makes the management of such data increasingly challenging for both users wishing to preserve confidentiality and forensic investigators attempting to establish reliable evidence.

This extended abstract describes the experimental design of an on-going investigation of the data contents of re-sold mobile devices. The consistency of results across different mobile forensic investigations is also investigated. The purpose of the experiment was to (a) estimate the amount and type of sensitive information retained on re-sold mobile devices and (b) the consistency of data recovery by standard commercial forensic applications.

1. INTRODUCTION

There are an estimated four billion mobile subscriptions globally, with a penetration rate of over 61% [3]. The increasing storage capacity of mobile devices means that increasing amounts of sensitive personal and corporate information may be collected on the device by users over the device's lifetime, often without the knowledge of the user. The complexity of modern devices means that ensuring the confidentiality of such information poses a challenge to individuals and organisations. Actions such as resetting the mobile device, removing the battery or re-storing factory default settings may appear to remove deleted files from a device's file system. However, it is unclear whether the corresponding file contents are actually deleted as well, or how much data can be recovered during forensic examination.

The same trends in mobile devices presents a challenge to legitimate forensic investigations of mobile devices. Evidence from mobile devices is typically obtained either *logically* through interaction with the device operating system, or *physically*, working directly with the device storage medium [1]. Physical extraction reduces the risk of altering stored data and avoids dependency on the fidelity of the operating system. However, physical extraction is generally more challenging because of the complexity and diversity of technologies used, the inaccessibility of the storage media without destruction of or damage to the device [4], and the difficulty of recovering information (files, objects etc) from raw data.

A number of software applications have been developed to enhance privacy of user information on mobile devices and conversely, to support the forensic extraction of data for investigation. There is limited research on the consistency of results between different forensic application vendors, or the effectiveness of privacy enhancing practices or applications. This extended abstract describes the experimental design of an on-going investigation of the data contents of re-sold mobile devices and the tools used to investigate them. In some respects, the work is similar to that of Garfinkel and Shelat [2], however we focus on the storage of information on mobile devices for the reasons outlined above.

The investigation was guided by two high level, complementary hypotheses:

H-confidentiality: sensitive data is retained on re-sold mobile devices (and is retained even following attempted deletions by a user); and

H-consensus: different mobile phone extraction software applications produced different forensic results

the purpose of the investigation is to report on the extent to which sensitive data can be recovered from re-sold devices using industry standard equipment, and to estimate the degree of consistency between the results produced by different mobile device forensic applications.

2. ACQUISITION

The first stage of the experiment was to acquire a sample of re-sold mobile devices. For the purpose of the experiment, a mobile device was defined as any electronic device with a GSM or 3G mobile capability, measuring less than 150mm by 100mm by 15mm. 50 devices were purchased from sellers on the auction website eBay[1] and paid for using a PayPal[2] account.

An eBay search was created in the *mobile phones* category, with the following filters applied: *used*, *UK only*, *buy now* and *with PayPal accepted*. The listings produced by the search were then filtered by one of the four price categories (including shipping) in the ranges 0.00-19.99, 20.00-39.99, 40.00-59.99 and 60.00-150.00 pounds. The listings were then sorted by time left for sale (least first) and the first device in the list selected for review. The listing was inspected for reports of damage likely to make data unrecoverable from the device. If the listing appeared satisfactory, the device model was checked against a list provided by the four forensics applications providers.

Discussion. We are aware that parts of the experimental design may have biased the results collected. For example, by selecting UK only sources, we restrict data collected to be largely from the United Kingdom; selecting PayPal accepted may exclude private sellers who prefer to be paid by cheque (small scale sellers may be less likely to use a payment clearing agency because of setup costs); the price ranges we have specified may not provided a representative sample of device usage. The results of the current investigation will inform the experimental design of future work.

3. INVESTIGATION

Three investigators were trained in the use of forensic applications. In addition, the investigators were trained in secure behaviour with respect to the confidentiality of mobile device data and required to sign confidentiality agreements concerning the information stored on mobiles. All work took place within a physically secured and network isolated room, during the period July – September 2010. Four desktop machines were setup in the investigation room. One of three forensic applications was installed on a different desktop machine: Cellebrite's Universal Forensic Extraction Device; XRY Forensics' Examination Kit; and Radio Tactics' Aceso, along with any accompanying hardware. In addition, SIM cards for major network providers were acquired.

Results from the investigations were stored on the spare desktop machine and a backup onto an external hard disk was completed daily. Each mobile phone was analysed using each of the forensic applications as follows:

1. Complete an initial survey of the device, recording the International Mobile Equipment Identity (IMEI) number, the date and time of the start of the investigation, handset serial number, manufacturer; colour and model.

2. Take photos to indicate general appearance, as well as any noticeable damage or alterations (front, back, serial number, SIM card).

3. Remove the SIM (if present) and any media cards.

4. Process the SIM by recording the International Mobile Subscriber Identity (IMSI), the Integrated Circuit Card Identifier (ICC-ID). and extracting any contacts and SMS messages.

5. Attempt the following two steps with (in order) no SIM card present, an Aceso cloned SIM card, the original SIM card or a generic vendor specific SIM card:

   - a physical acquisition of data stored on the handset using UFED and then XRY
   - a logical acquisition of data stored on the handset using UFED, XRY and Aceso
   - a manual inspection of the device contents via the user interface

   this ordering of work was adopted to minimise potential for alteration of device contents resulting from interactions between the device and the SIM card.

6. Analyse the data recovered, recording the number of information artefacts (SMS messages, emails, contacts, etc.) and classifying them as personal or corporate and indicating whether the information could be regarded as sensitive.

Each phone was independently re-examined a second time by a different investigator, and a final investigation report was produced as an agreement between the two results.

All data recovered from the mobile devices was stored in a database for subsequent review and analysis.

4. SUMMARY

This extended abstract has described the experimental design for an investigation of the data contents of re-sold mobile devices. The work will also investigate the variability of evidence produced between different mobile forensic application providers. Preliminary results of the work will be presented at PUMP in the autumn of 2010.

5. REFERENCES

[1] R. Ayers and W. Jansen. Guidelines on cell phone forensics. Special Publication 800–101, National Institute for Science and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, May 2007.

[2] S. L. Garfinkel and A. Shelat. Remembrance of data passed: A study of disk sanitization practices. *IEEE Security and Privacy*, 1(1):17–27, January 2003.

[3] J. Q. Pearce. Report: 4.1 billion mobile subscribers worldwide helps reduce digital divide (slightly). `http://moconews.net/article/419-4.1-billion-mobile-subscribers-mobile-helping-reduce-digital-divide-sli/`, March 2009.

[4] S. Willassen. Forensic analysis of mobile phone internal memory. In M. Pollitt and S. Shenoi, editors, *Advances in Digital Forensics. IFIP International Conference on Digital Forensics*, pages 191–204, Orlando, Florida, USA, 2005. Springer.

[1] `http://www.ebay.co.uk`

[2] a payment clearing subsidiary of eBay, `http://www.paypal.com`