Mobile Forensics for Cloud Data: Practical and Legal Considerations

John Bjornson
School of Computing and Academic Studies
British Columbia Institute of Technology
Burnaby, BC, Canada
Email: john.m.bjornson@gmail.com

Aaron Hunter
School of Computing and Academic Studies
British Columbia Institute of Technology
Burnaby, BC, Canada
Email: aaron_hunter@bcit.ca

***Abstract*—Forensic examinations of a mobile phone that consider only the internal memory can miss potentially vital data that is accessible from the device, but not stored locally. In this paper, we look at a forensic tool that is able to download data stored on the cloud, using credentials gleaned from device extractions. Through experimention with a variety of devices and configurations, we examine the effectiveness of the software for its stated purpose. The results suggest that we are able to obtain information from the cloud in this manner, but only under some relatively strong assumptions. Practical issues and legal considerations are discussed.**

I. Introduction

Digital forensic tools have traditionally been used by law enforcement agencies to help with criminal investigations by extracting data from computing devices. Over time, the emphasis has shifted from data stored on personal computers to data stored on mobile phones. In both cases, the process is similar: a forensic image is obtained from the device in a manner that does not modify the data, and then information is obtained from this image using suitable software. This process involves specialized hardware and software, the reliability of which has been an important focus for the forensic community[3]. However, simply extracting data from a device is no longer sufficient. A great deal of important information is now stored on the cloud, so a traditional forensic image does not capture everything an investigator needs to know. In order to address this issue, we need to move beyond the device to obtain information that is stored remotely.

In this paper, we evaluate a new tool for obtaining cloud-based information associated with a mobile device. We make two contributions to existing research in digital forensics. First, while the importance of cloud data is widely known, it is generally hard to know how effective tools will really be in the field. Through contacts at the Royal Canadian Mounted Police (RCMP), we were able to obtain a variety of real discarded mobile phones for testing. This provides us with a more accurate assessment of utility. It is worth noting that the device evaluated in this document is currently available for law enforcement, but it can not be sold to academic institutions. The second contribution of this paper is a preliminary discussion of the legality of the process. The challenge in dealing with cloud data is that information sources must be accessed quickly before data can be deleted. This raises important questions around the notion of search and seizure.

II. Background

A. Data Extraction

Cellebrite's Universal Forensic Extraction Device (UFED) line of tools and applications is widely used today by the digital forensics community, including law enforcement. The UFED Touch is hardware that supports acquiring data from mobile devices. There are several different levels of extraction. The lowest-level form is a physical extraction, which essentially creates an exact copy of memory of the mobile device [1]. The tool also supports file system extraction, which simply replicates the files and data on the device. This not only includes standard files like images and video, but it also includes things like passwords and message logs.

Upon completing an acquisition using the UFED Touch, the resulting data can be opened by UFED Physical Analyzer for decoding and analysis. Physical Analyzer essentially exports the data obtained to a readable format, such as Word, Excel or PDF. Additionally, in cases where the UFED Touch does not itself provide native support for extracting data from a device, Physical Analyzer offers the ability to bring in data extractions such as flash memory dumps for analysis. This is useful in cases where advanced techniques such as Joint Test Action Group (JTAG) or physical removal of the flash memory chip (chip-off) from the printed circuit board (PCB) are needed to acquire data from a mobile device. With this flexibility and functionality, Physical Analyzer has grown to become an invaluable tool for forensic examiners.

B. Cloud Analyzer

In 2015, Cellebrite introduced UFED Cloud Analyzer, which takes data extraction beyond simply what is stored on a device's physical memory [2]. Using login credentials gleaned from a device extraction, Cloud Analyzer attempts to download private user data stored on connected cloud services. In cases where on-device encryption or limited caching of application data might once have served to restrict the amount of recoverable information from local storage, having the ability to download the full content of a users cloud data

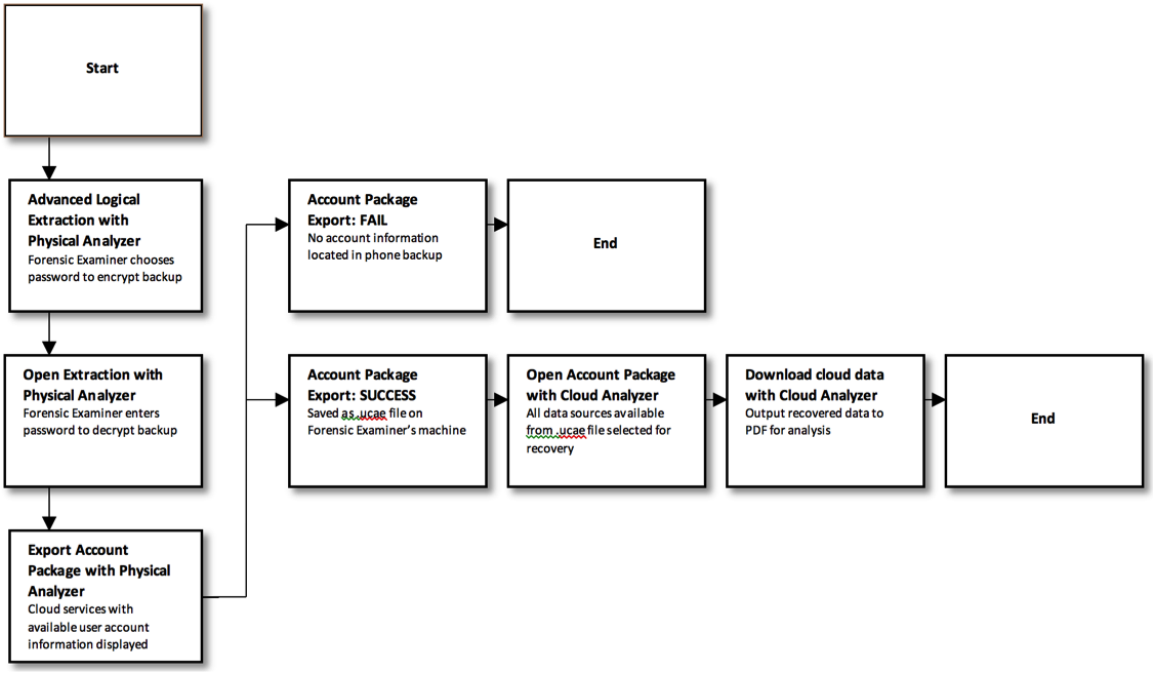

Fig. 1. Work Flow

now has the potential to yield far more information than was previously available.

At present, Cloud Analyzer attempts to obtain data from Facebook, Twitter, Gmail, Dropbox, Google Drive, Kik and Google Location History. These are all applications that users install, and then store login credentials on the device so that they can be opened with a simple tap. Since the login credentials are stored locally on a device's internal memory, Physical Analyzer can try to recover them. If retrieved, these login credentials can be utilized by Cloud Analyzer to access and download data stored in the cloud for the applications it supports. The software actually automates this process, returning all available information from the cloud in the returned result.

Note that Cloud Analyzer can not be used to obtain information from applications where the login credentials are not stored on the device. This is the case, for example, with mobile banking applications that are developed with a security-first focus instead of prioritizing convenience for the user.

The focus of this research is to test how effective Physical Analyzer is at recovering username and password information from iOS and Android device extractions, and subsequently how successful Cloud Analyzer is at using these credentials to access the respective cloud accounts.

III. Accessing Cloud Data

A. Approach

We take an experimental approach, using Cloud Analyzer on the iPhone 6 and the LG G3 smartphone. The general stages for a complete test run after setting up a device involve performing a device extraction, exporting an account package from the extracted data, and then importing the account package into Cloud Analyzer for attempted recovery of cloud data. We tested each device with encryption disabled first, then with encryption enabled. In this manner, we can identify whether or not encryption has an effect on the Device Extraction, Account Package Export, or Cloud Data Extraction stages.

The basic process for each test run is given in Figure 1, although there is some minor variation between different devices.

B. Results

As stated previously, full physical extraction is the preferred approach. However, in the process of examination, we determined that that physical extraction is not possible on iPhone 6. As such, we were restricted to a logical extraction of the file system. Neverthelss, in each case, we were able to perform the extraction, and successfully pass the result to Cloud Analyzer. Cloud Analyzer returns any credentials that are present for any of the supported cloud services. There is an important caveat here, however. During the extraction, Physical Analyzer actually required the examiner to enter the device passcode and the encryption password. Without this information, the user credentials will be encrypted and unusable by the investigator.

The UFED Touch supports a physical extraction from the LG G3 smartphone through two methods. The first method is Bootloader mode in which a custom bootloader is uploaded to the phone that allows for downloading the full contents of the phone's internal memory. This is the recommended mode by Cellebrite, and there is no need for the Forensic Examiner to know the passcode for the device due to the OS never being loaded in the extraction process. The second

	ENCRYPTION ENABLED	ACQUISITION TYPE	ACCOUNT PACKAGE EXPORT	CLOUD ANALYZER RESULT
TR1 | IPHONE 6	No	Advanced Logical	Success	Success
TR2 | IPHONE 6	Yes	Advanced Logical	Success	Success
TR3 | LG G3	No	Physical (Bootloader)	Success	Success
TR4 | LG G3	Yes	Physical (Bootloader)	Fail	Fail
TR5 | LG G3	No	Physical (ADB with root)	Success	Success
TR6 | LG G3	Yes	Physical (ADB with root)	Success	Success

Fig. 2. Results

physical extraction method available on the UFED Touch is Android Debugging Bridge (ADB) mode. In this mode, the examiner must enable USB Debugging on the device, which is done manually on the phone after the OS has booted and the passcode has been entered. In addition to knowing the passcode to facilitate this, root access must also be gained to the device to allow for a complete download of the internal memory.

Since there are two methods for extraction, we actually had four trials on the android phone. We attempted the extraction with the Bootloader method, first without encryption and then with encryption. We then attempted the extraction with root access, with and without encryption. Of these trials, three were successful in the sense that they returned credentials and allowed us to obtain the information available on the cloud. The one trial that was unsuccessful was the Bootloader method with encryption. In this case, although we had the passcode for decryption, we were never prompted to provide it during the extraction process. As a result, the software actually failed; we were unable to complete the Bootloader extraction on an encrypted Android phone.

The basic results are summarized in Figure 2. The table indicates that the extraction was a "success" in five cases out of six. While this is true, it is important to keep in mind the information required in each case. For the iPhone cases, we needed a device passcode and encryption password. In the final two cases, we needed a pass code and root access to the device. The most successful instance, therefore, was the case labelled TR3. This was the case in which data was unencrypted on an android device. In this case, we were able to obtain user credentials even without the passcode.

IV. Legal Considerations

A. Overview

It is generally believed that mobile devices provide more information to an investigator per byte examined than a computer [5]. Having the ability to acquire this information from a phone and the associated cloud services is therefore a top priority for law enforcement. The problem is that a forensic examination of a seized mobile device could potentially yield access to terabytes of data stored on servers physically located in another country. Should this be the case, jurisdictional challenges arise, as well as a heightened expectation of privacy concerning the data being accessed.

B. Search and Seizure

The main legal issue to consider is the protection that citizens have from unreasonable search and seizure. This protection is granted in Canada by the Canadian Charter of Rights and Freedoms; it is granted in the United States by the Fourth Amendment to the Consitution. There have been well-known criminal cases in which individuals have been acquitted because evidence has been improperly obtained from computers or cell phones.[1] It has also been noted in court that we need to be careful about the fact that data extracted from computers may generate detailed information about an individuals interests and habits without consent [6]. This concern is particularly problematic when we use something like Cloud Analyzer to access private social media data.

Kruglick emphasizes the importance of the integrity of the data gathering process [4]. This is a key issue for cloud data, because most of it is accessible from any computer or smartphone with an internet connection. This can create the need to acquire cloud data quickly in order to prevent it from being modified. Demonstrating that the data is collected in a safe and timely manner is an important step. However, we need to specify exactly what this means in a manner that respects the criminal code; or else we need to argue pursuasively that the criminal code needs to be modernized to address data on cloud services.

While it may seem obvious that data on the cloud could be relevant to any given investigation, it is important to note that case law is generally a step behind the technology when it comes to dealing with search and seizure of electronic devices. Laws are slow moving and occasionally outdated; enforcement can be further complicated by jurisdictional boundaries, when cloud data is stored across state or provincial lines. As such, there are currently few examples of case law that serve to definitively set the standard for when the forensic examination of a mobile device can or cannot be extended to include cloud data.

A thorough legal review is outside the scope of this document, but such a review would be an important step in determining when we can safely use Cloud Analyzer in

[1] See, for example, [7].

a particular jurisdiction. As noted previously, the situation is currently so unclear that Cellebrite will only sell Cloud Analyzer to verified law enforcement users.

C. International Concerns

Note that we have focused entirely to this point on the domestic issue of unreasonable search and seizure. There is clearly another problem with respect to obtaining cloud data that belongs to someone else, and exists on a machine in a foreign country. In an ideal setting, Cloud Analyzer would know the applicable laws as well as the physical location of cloud data. This is not a reasonable expectation in the short run, so we are left leaving individual investigators with the responsibility of respecting foreign laws. This is clearly a situation that is open to violation and abuse.

V. Conclusion

In this paper, we have looked at Cloud Analyzer, which is a tool that extends the forensic investigation of a mobile device to include data on the cloud. We have suggested that this is an important capability, but there are both technical and legal issues to be addressed in practice.

The results of our preliminary testing demonstrate a major problem faced by law enforcement agencies in dealing with cloud data. In most cases, it is unlikely that the passcode for the phone will be known in advance. As such, the only case where we are likely to be successful is the android case using the Bootloader. But even then, the utility of Cloud Analyzer is dependent on the lack of encryption. If we are given a phone with no encryption, we can presumably find the credentials for the given applications through manual inspection. Of course, there is still value in a tool that bypasses the passcode, and automatically compiles the available cloud information; but it is clear that more work is required to fully handle cloud extraction from a mobile device.

In terms of legal concerns, we focused on the lack of appropriate case law related to search and seizure. However, this is clearly just one area of concern. There are international jurisdiction issues to be addressed as well, and we need to educate both investigators and judges on the best practices for maintaining the integrity of cloud data. It is clear additional research on the legal considerations must be carried out before this new technology can be employed safely.

Although our work is largely just a simple test of a new tool, we remark that this particular test is unique in the academic literature. Not only is Cloud Analyzer a new tool, but it is one that is currently not available for academic use. We are therefore in a strange situation at present, where law enforcement officers are using a tool to gain access to data, without a clear view of the legal issues at play and without open external testing. Our aim in this paper was to make this issue clear, and to provide first steps towards a proper evaluation.

References

[1] Cellebrite Mobile Synchronization Ltd. (2014). Cellebrite On-Line Documentation, (http://lang.cellebrite.com/mobile-forensics/capabilities/operations/physical-extraction), accessed 2015.

[2] *Extracting Legally Defensible Evidence From The Cloud*, (http://www.cellebrite.com/Media/Default/Files/Forensics/White-Papers/Extracting-Legally-Defensible-Evidence-From-Cloud_WhitePaper.pdf), accessed 2015.

[3] S. Danker, R. Ayers, and R. Mislan. Hashing Techniques for Mobile Device Forensics. *Small Scale Digital Devie Forensics Journal*, 3 (1), 1-6, 2009.

[4] K. Kruglick. *A Beginner'sPrimeron the Investigation of ForensicEvidence*, (http://www.scientific.org/tutorials/articles/kruglick/kruglick.html, accessed 2016.

[5] J. Lessard and G. Kessler. Android Forensics: Simplifying Cell Phone Examinations. *Small Scale Digital Device Forensics Journal*, 4(1), 2010.

[6] *R. v. Fearon*, 35298, Supreme Court of Canada, 12/11/2014.

[7] *R. v. Vu*, 34687, Supreme Court of Canada, 11//07/2013).