Mobile Device Forensics: Beyond Call Logs and Text Messages

Daniel Ogden
Senior Digital Investigative Analyst
Cybercrime Lab
Computer Crime & Intellectual Property Section

I. Introduction

Throughout the year 2016, the Computer Crimes and Intellectual Property Section (CCIPS) Cybercrime Lab saw an increase in the number of supports and inquires relating to mobile devices. These inquiries include questions about how data is stored, whether the data is recoverable, and whether you can get the data if the device is locked.

As we all know, the mobile device market, which includes cellphones and smartphones, is rapidly growing. The market growth has allowed manufacturers to create thousands of different phone models we see in use today. These different models have brought many challenges to examiners when tasked with extracting and analyzing data from mobile devices. The technology involved with mobile devices is also advancing, which allows manufacturers to release new models of phones each year, with thinner cases, better graphics, faster processors, more storage, and yes, better security features.

Since the release of the first smartphones, Apple's original iPhone (running iPhone OS) and HTC's Dream G1 (running Android 1.0), consumers entrust their lives to mobile devices. In a 2015 survey conducted by the Pew Research Center, 92 percent of people in the United States owned a cellphone, and 68 percent owned a smartphone. PEW RESEARCH CTR., DEVICE OWNERSHIP (2015). That averages out to almost one mobile device per person in the United States.

How does this effect law enforcement? With mobile devices allowing consumers to communicate, socialize, bank, shop, navigation, start their car, track their health, and monitor their in-home surveillance cameras, a plethora of information is contained on these devices. Just about every crime being committed has the potential to have the involvement of a mobile device, but the investigation team must first recognize the mobile device—whether it is a watch, phone, or tablet—and then preserve the data for collection and analysis. While it is getting more difficult to bypass security features in mobile devices, the Cybercrime Lab can assist you in determining your options.

II. Preservation of data

For all investigators, identifying and preserving data is the goal when seizing digital evidence. This can be more difficult when dealing with mobile devices that have their own distinct challenges different from the laptop and desktop computers. One challenge is knowing what to look for. With smaller and novelty devices on the market, such as the BMW style key fob mini phone, it makes identifying the devices more difficult. Another challenge is collecting all of the data. While mobile devices store a lot of data, the extraction of data from the device may be missing important evidence. Not all data is stored on the device, even though the user has access to the data. With the ease of cloud computing, companies such as Dropbox, Microsoft One Drive, and Google Drive provide the user with capabilities to create, transfer, receive, and delete data in the palm of their hand. While the user may have access to this data from their mobile device, it may not be recovered during extraction and analysis due to data being stored in the cloud or on remote storage. Therefore, it is imperative for the investigative team to determine what web-based email accounts, social media accounts, and file storage the user may have so the accounts can be preserved. This data, along with the extracted data from the mobile device, could paint a better picture of what occurred during a timeframe.

III. Extraction

One of the most common questions received in the Cybercrime Lab is if the data can be extracted. This is an ever-changing answer because locked devices that cannot be unlocked today may be unlocked next week. As tools vendors work at developing methods to acquire data from devices that are unsupported, they release updated versions unlocking and decoding new devices several times a year. These updated versions may support a device sitting in evidence collecting dust. It is recommended that stored evidence items should be re-evaluated every few months to see if they are covered in a released update. If the device is not supported with commercial tools, you can contact the Cybercrime Lab (cybercrimelab@usdoj.gov) for assistance in determining what options are available. The lab will ask you to provide the make and model number from the device, operating system if known, and the carrier (i.e. Samsung, SM-G900P, Android 5.1, Sprint).

There are different levels of data extractions from mobile devices, just as with computers. Some allow for further, deeper analysis, and some do not. Knowing which type of extraction was completed is important and can be derived from the report. The three common extractions are Logical, File System, and Physical.

A Logical extraction is the quickest of extractions, and extracts the data through issued API (Application Programming Interface) commands. The commands allow the device to return the requested information from the device, such as the contents of SMS, call logs, and media, but not typically data from the third-party applications. Typically, the File System extraction will include the file structure of the device, collecting the folders, sub-folders, and their data. This generates more data than the Logical extraction, and can be used for further examination—the deep dive. The Physical extraction is the most comprehensive of the extractions. This will provide a bit-for-bit copy of the device’s flash memory. With this, you will have the entire memory capture, including the unallocated or deleted space and hidden system files that the user does not see.

With locked devices, the Cybercrime Lab uses various techniques and tools to acquire the data. If your device is listed as unsupported, contact the Cybercrime Lab at Cybercrimelab@usdoj.gov for assistance.

IV. Analysis

One key benefit in obtaining a file system or physical extraction is the ability to perform advanced analysis of the device data. This includes the data contained inside the applications, more commonly called apps, that are installed on the device. Apps are self-contained software programs either pre-installed or user installed on the device to run programs such as messaging, GPS, social media, and web browsers. The data in these apps is typically stored in SQLite databases and often contains valuable information.

During the analysis of the data, SQLite databases on the device are identified by their file header, 0x53514C69746520666F726D6174203300. The known databases are identified, decoded, and presented to the examiner in a readable, organized format. In commercial tools, the data is read from the SQLite databases and separated into unique sections—such as SMS, Call Log, and Contacts—for the end-user. Known databases are those that the tool has been programmed to recognize and understand how the data is stored. The commercial tools support and decode thousands of different apps, including the popular social media, communication, file storage, and mapping applications, but the databases may need to be exported for further analysis.

What if the entry or data was deleted? Depending on the configuration of the database and its associated files, the data may be recoverable. Some SQLite databases have associated WAL, or Write-Ahead Log, files to assist in writing data to the database. As entries are written by the user, such as a contact entry or SMS message, they are first written to the WAL file. The database will check for the most current data, which either resides in the database or in the WAL file. The data is then moved from the WAL file to the database once the database has completed a normal shutdown. But is the data still in the WAL file? Yes, it could be. SQLite forensic tools, such as Sanderson's SQLite Forensic Suite, allow examiners to search the database and the WAL file for deleted entries that are no longer visible to the user and some commercial tools.

To help explain this, here is an example: if there were five contacts in the Contacts_2.db (.db signifying a database) and I deleted one, the database itself would only see the four remaining entries. If I add a new contact entry but the database failed to close properly, I would still have only four entries.

The new entry would have been in the WAL file, and if the tools failed to process the WAL file, the data could have been missed. However, if I allow the new entry to be added into the database, this could overwrite old data that was present and set to be updated with the new entry. If there is a question about data, or missing data, from a database, and there is an accompanying WAL file, the best practice is to use tools designed for SQLite analysis. A deeper dive into the database may recover old entries that are no longer seen by the database, as well as possibly indicate when the entry was present.

Other challenges with mobile devices are the number of different apps and ensuring that those apps are being supported in the report. We discussed above about "known" databases, but what about unknown databases, those that are not supported for decoding. An example of data not being decoded occurred during the analysis of a physical extraction from a Samsung device. The analysis for Blackberry Messenger revealed a Blackberry Messenger database at this file path: /Root/data/com.bbm/files/bbmcore /master.enc. The database was not decoded due to the database being encrypted, evident by the master.enc file and the data being unreadable (hexadecimal, 0xF6F7CBD9CC1E1D8933392F, which translates to "……..30/"). The physical extraction allowed for the recovery of the keys to decrypt the database, and once it was decrypted, the database file signature was visible (0x53514C69746520666F726D6174203300 translated to SQLite format 3), and it revealed 1,579 chat messages.

V. Conclusion

Mobile devices contain more than just call logs and text messages; they contain a plethora of information, some in the device and some in the cloud. Working with the investigative team to locate and preserve the cloud and web-based accounts will help provide a better picture of the subject's life.

With your locked devices, remember that if it is not supported today, check back or contact the CCIPS Cybercrime Lab for updates and possible solutions. With this ever-changing time, devices not supported last week could be supported next week.

Most mobile device forensic reports come with a list of application SQLite databases identified on the phone. This list needs to be reviewed to see if the database was decoded. While it is not common for commercial tools to miss supported databases, an update from the app builder could influence whether the tool worked properly. Third-party tools can assist in looking deeper into databases if the need arises. If you need assistance with your mobile device, contact the CCIPS Cybercrime Lab for assistance at CybercrimeLab@usdoj.gov.

ABOUT THE AUTHOR

❑ **Daniel Ogden** is a Senior Digital Investigative Analyst in the CCIPS's Cybercrime Lab. He has over 22 years of law enforcement experience and 12 years in the computer crime profession. He is a Cellebrite instructor and specializes in mobile device analysis and computer forensics. He previously served as a Computer Crime Investigator with the Brevard County Sheriff's Office and served 11 years on federal task forces investigating computer related crimes.

The Cybercrime Lab is a group of highly trained digital investigative analysts located in the Computer Crime and Intellectual Property Section of the Criminal Division in Washington, DC. The Cybercrime lab provides support to prosecutors through advanced digital investigative analysis, technical and investigative consultations, and research and training in support of Department of Justice initiatives.