Mobile devices, including smartphones and tablets, have become essential within today’s society in both personal and professional settings. Sometimes the lines between personal and company data become blurred when individuals use their work devices for personal uses and vice versa. In the event of an investigation, that data will be highly sought after.

These devices vary in design and are continually undergoing changes as existing technologies improve and new technologies are introduced. Due to this, the practice of mobile device forensics includes many approaches and concepts that fall outside of the boundaries of traditional digital forensics. Examiners responsible for mobile devices must understand the different acquisition methods and the complexities of handling the data during analysis. Extracting data from a mobile device is half the battle. The operating system, security features and type of mobile device will determine the amount of access the examiner will have to the data.

Over the past decade, mobile devices have become significantly more sophisticated providing speed, storage capabilities and technologies matching or even beating that of personal computer and laptops. It is widely accepted that most individuals, including children, own or have access to a mobile device. In fact, the number of active mobile devices totals more than seven billion.[1]

We all use them on a day-to-day basis and they have therefore become an incredible tool for storage of personal information and data, giving great insight into a person’s life. It is for these reasons that mobile devices are becoming very valuable sources for evidence. In many instances, a mobile device is the only source of digital evidence available for tracing an individual’s movements and motives. It can help answer questions such as who, what, when, where, why and how.
Mobile devices contain a myriad of potential sources of intelligence and evidence for an investigation.

The following are types of personal information and data commonly stored on mobile devices:

- **Application and communication data**: Communication data consists of data such as contacts, call logs, messages, chat data, emails and social media accounts. Application data refers to the information stored within third party applications on the mobile device, for example Facebook, LinkedIn, Uber, Dropbox and mobile dating applications. This information can amongst other things, help establish communications between an individual and external entities. It can also identify an individual’s family members, friends, acquaintances and foes. The data can be used to develop a network of a person’s “close associates,” which can assist with certain types of investigations, such as: conspiracies or cartel activity where more than one individual is involved.

- **Multimedia files**: Large storage capacities in mobile devices can result in thousands of pictures, videos, music files and other media being stored. Such files can be used as evidence in an investigation as an examiner is able to trace their origin and discern if it was received from an external entity or downloaded from the internet. With modern mobile devices, location-based data is often embedded within media files, unbeknown to the user. By utilising appropriate forensic techniques, this information can be accessed and presented.

- **Internet history and email**: Internet capability on modern day mobile devices can rival that of many computers. A more advanced mobile device will additionally store an internet history, internet cache, internet bookmarks and email. Email, internet browser history and bookmarks can provide great forensic insight, and mobile devices provide another source of this data.

- **Location data**: Various location tracking technologies implemented in mobile devices can provide valuable information in an investigation. When a person is travelling, for example, their mobile device could be connecting to roaming networks, Wi-Fi hotspots, cell site towers, etc. Each of these actions leave a “footprint” of locations that a person has visited. Such information is very valuable to an investigation when trying to place an individual at a certain location where an incident is known to have taken place. It is also possible to track when and for how long the mobile device was placed on charge in a given location.

- **Malware**: Like computer systems, mobile devices are also vulnerable to malware. Forensic tools can detect malware on mobile devices. Further analysis can help uncover what effect the malware has on the mobile device and to understand if sensitive information was pilfered from the device or if a third party was monitoring communications.

- **Backup and cloud data**: Due to the portable nature of mobile devices, the risk of data loss increases as the physical device may be stolen, go missing or malfunction. Many individuals choose to either backup their device locally (to a PC) or to back
up their device to a cloud service to reduce this risk. These backup sites can host a wealth of information (sometimes even more than the actual device) as multiple historic backups can be stored and subsequently accessed using forensic techniques.

**Personal Data or Company Data – Who Is Legally Responsible?**

There are many legal aspects of corporate investigations to consider. For example, it is difficult to determine to whom the data belongs if an employee backed up their device to a corporate laptop and the contract of employment states that all data on the corporate laptop belongs to the company. When situations like this arise, organizations should obtain professional legal advice to prevent costly mistakes.

**Proactive Actions to Preserve the Data**

If a mobile device or similar accessory becomes potentially relevant to an investigation, then it is important that it is handled in the correct manner from the very start. The below best practices will help to preserve the evidential integrity (and therefore future use) of the data from these types of devices:

i. **Immediately place the mobile device in airplane mode.** Many modern mobile devices can be wiped remotely. Placing the device in airplane mode effectively means that the device is unable to connect to any network which makes it impossible to remotely wipe.

ii. **Document the pin code and user’s credentials.** Even though there may be some situations where a digital forensic practitioner would be able to bypass the pin lock code, it is always better to document the pin lock code from the user. Should the cloud backup need to be collected, the user’s login credentials for the cloud backup service (iTunes, Gmail, etc.) would also be required. When in doubt, obtain as many credentials as possible as it is unknown what type of data the investigation may require.

iii. **Enquire as to how the user backs up their data.** Ask whether it is hosted locally, to the cloud, or both. It also may be useful to question which charging method is used. Often a backup will occur without the user’s knowledge when charging via connection to a computer.

iv. **Thoroughly document the device, noting all information available.** Be sure to use photography to support this documentation.

**Data Capture – Four Levels of Access from Logical to Manual**

To gain access to the data held on mobile devices, the data must first be captured following forensic principles. There are many different methods of achieving this and the method employed will depend on the make, model and operating system of the device in question. These different data acquisition methods also dictate which recovery techniques should be applied, as detailed below:

i. **Logical Acquisition:** A logical data acquisition from a mobile device means that a bit-for-bit copy of “logical storage objects” is extracted. Logical storage objects include files and directories that reside on logical storage (file system). A logical data acquisition will not normally produce any deleted data, as it is normally removed by the mobile devices file system. The amount of data resulting from a logical acquisition is typically much less comprehensive than that which is available from a file system or physical extraction.

ii. **File System Acquisition:** A file system extraction is a type of logical extraction which also extracts the files embedded in the memory of a mobile device. Mobile devices that run on popular operating systems such as Android and iOS are built using a SQLite database platform. When data is stored in a SQLite database on a mobile device and data is deleted, the data is not overwritten. When data is deleted in a SQLite database it is usually marked as deleted and made available to be overwritten later. A file system extraction from a mobile device also has the advantage of showing the file structure, application data, web artefacts as well as allowing the forensic examiner to perform the analysis using tailored tools and scripts.

iii. **Physical Acquisition:** A physical data acquisition from a mobile device means that a bit-for-bit copy of physical storage is extracted. This would give a forensic examiner a bit-for-bit copy of the mobile device’s flash memory; similar to the way
data is acquired in traditional computer forensics. A physical data extraction extracts the data directly from the mobile device’s flash memory(s). After the data is extracted, the memory dump is then decoded. This type of extraction enables the maximum amount of deleted data to be recovered.

iv. Manual Acquisition: This involves using the mobile device’s interface to investigate the data stored on the device. An individual will use the mobile device as normal, taking pictures or videos of the content displayed on screen. Data can also be captured by connecting the mobile device to a computer using an AV adapter and taking screenshots of the device as it is navigated. This is a very invasive technique of acquiring the data and should only be used once all other acquisition techniques are exhausted.

Case Study: A “Last Resort” Success Story

To provide an example of what can be achieved, A&M recently completed a case involving a Samsung Galaxy S7 mobile device. The device was provided to us after being wiped clean whilst another entity tried to recover the passcode. Local law enforcement had also given up on trying to recover the deleted data. Utilising advanced methods, A&M was able to communicate with the device via a command line interface and thereafter utilised the device’s onboard operating system to physically image the device directly to a computer. Using this approach, A&M recovered large volumes of data including deleted chat messages, SMS messages, call logs, etc. This was not thought to be possible previously. Because this method is somewhat intrusive, it should only be used as a “last resort.”

Conclusion

Since mobile devices are popular platforms for various applications, they can offer imperative evidence in forensic investigations. These devices often serve as a source of digital evidence in crimes and contain personal information about an individual, such as photographs, passwords and other useful data. Mobile devices also show where individuals are located at a specific time and with whom they were communicating. The information contained in mobile devices can also be instrumental in the investigation of a crime when they are used to steal intellectual property. For these reasons, mobile devices must be thoughtfully considered in any investigation – especially given their recent proliferation.

[1] Groupe Spéciale Mobile Association

Source URL: https://www.alvarezandmarsal.com/insights/your-mobile-device-best-piece-evidence-investigation

Links:

Authors: Phil Beckett, mailto:pbeckett@alvarezandmarsal.com, +44 779 873 3555
Graeme Buller, mailto:gbuller@alvarezandmarsal.com, +44 207 663 0567