iForensics: Analyzing Apple Watch Data

Robert C.

[redacted]

Abstract

Digital and mobile devices have exploded in popularity in the last ten and twenty years to say the least. With the expansion and wide adoption of mobile devices in mainstream society, wearable technology like smart watches has become a normality in our modern world. Wearable technology is so commonplace that most people forget about how much data the devices can and are always capturing. For this reason, it could be crucial during a forensics investigation for examiners to confiscate the suspects smartwatch or other wearable technology, because a lot of information can be gathered from the device alone and the suspect likely has not taken precautionary measures they usually take on said device.

Mobile devices have been around since as early as the 1970s and have since developed to become very lightweight and portable devices overall. They now capture more data than everyday civilians could ever imagine. The average modern-day mobile device captures data from its various onboard or embedded sensors (microphone, camera, GPS, etc.). From these sensors, a lot of information about the user can be determined. However, it doesn't just span the physical world; mobile devices (and any computing device in general) capture several other data points such as the users' internet browsing history, logon history, and much more. Therefore, it's only natural for end-users to be worried about what data their seemingly personal and private devices are capturing and sending off to a remote location. Furthermore, the issue because amplified, but people seem to forget about it when discussing the data captured from any type of wearable technology such as a smartwatch. For example, the Apple Watch is easily the most common and popular smartwatch worn by everyday consumers on a daily basis with "over 43 million Apple Watches sold in 2020 alone" (Curry 2021).

With the Apple Watch initially being released in 2014 and since then having seven different iterations, it's safe to say that the Apple Watch has had its form of success. People are extremely excited to always have such smart technology so easily reachable on their wrist, but all of this doesn't come at some form of risk or cost. Every day civilians don't realize how much data is being passively captured by these extremely mobile and portable devices. The Apple Watch collects a surprisingly extensive amount of data from its seemingly unknowing users and it's one of the more conservative devices so say the least. The Apple Watch will collect data such as heart rate information, GPS information, text messages (from the paired iPhone), synced photos (from the paired iPhone) just to name a few. The way the Apple Watch works is it syncs data with the paired iPhone upon pairing with said iPhone and periodically while it's currently paired with that iPhone. However, the data that's being captured directly from the watch is stored on the

watch temporarily before making its way to the paired iPhone. Therefore, if a forensic investigator, law enforcement officer, or other appropriate authority, only has access to the Apple Watch of the criminal/crime scene (which is something very easily forgotten about in terms of 'covering your tracks), then the authority can pull a significant amount of information from the Apple Watch directly without having access to the previously paired iPhone. Some examples of data that could be pulled from the Apple Watch without having access to the previously paired iPhone are apps installed on the watch, WiFi logs for the device, photos synced with the device, and more.

Collecting the previously referenced evidence is always the hardest part of any forensics investigation and mainly consists of ensuring the devices in question aren't going to be tampered with in any way. After ensuring any kind of airplane mode, or internet-enabled access is disabled and the device is completely cut off from the internet, the data analysis and retrieval may begin. There are three methods for collecting data from an Apple Watch: "Logical extraction, File system acquisition, and cloud data acquisition" (Katalov 2019). In order to retrieve data from the device, a special device can be plugged into the ports that are accessible behind the watch bands. From there, the examiner pairs the Apple Watch to an iPhone (it can be any iPhone) and launches iTunes, then the Apple Watch will be available for viewing on the PC. Through utilizing various forensics tools like Elcomsoft, and iBackupBot examiners pull the data they need from the Apple Watch in question. Some items to note here are that the Watch OS does not have any native backup mechanism or service, so information must be pulled somewhat manually; and that there are no over-the-air data acquisition techniques for the Apple Watch except for (of course) iCloud acquisition. Lastly, backups from the watch are automatically created when the watch is connected to an iPhone and synced to the paired iPhone.

Utilizing those special tools mentioned earlier, examiners are able to extract apps that were installed on the device, get logs from the device, and transfer media files that were stored on the device from syncing the Apple Watch with the paired iPhone. Storage locations for data on the Apple Watch are for the most part in similar places for similar data types, making it fairly easy for forensic investigators to manually gather data from the device. Some specific areas or locations of interest for data found on the Apple Watch include:

- \mobile\library\deviceregistry.state\secureProperties.bin - for specific identifiers of the Apple Watch
    - Serial Number
    - UDID
    - WiFi MAC address, etc.
- \homedomain\library\deviceRegistry.state - 3 files of interest
    - HistorySecureProperties.plist
    - StateMachine.plist
    - History.plist
- NanoMail\registry.sqlite
    - Synced_account table – email accounts synced to the watch
    - Mailbox table – specifc emails in folders for each email account on the device
- Nanopasses\nanopasses.sqlite3 - transaction history from the watch
- NanoPreferencesSync\backup\files\ - media (pictures) stored on the watch
    - End-user pictures
    - Watch faces, etc.

It’s important to note here that the ‘.plist’ files are Apple proprietary “property list” files meant to hold various data types in them. So, how do investigators actually retrieve the data from

the Apple Watch itself? By making use of the tools briefly mentioned earlier – Elcomsoft iOS Forensic Toolkit, iTunes, and iBackupBot. Examiners will use Elcomsoft to retrieve data directly from the device by using "the 'I' (information) option to extract device info" (Epifani 2019) and produce three files upon initially connecting the device to a computer – ideviceinfo.plist, application.txt, and applications.plist. Then, use the 'M' command to get media information from the device. Collect images and other media synced from the paired iPhone (current or previous) by looking in the DCIM folder of the files produces. Some other logs that can be gathered from the Apple Watch device are power status logs(gathered through Sarah Edwards open-source toolkit APOLLO) and Wi-Fi logs – which could be used for location tracking purposes in conjunction with GPS logging information. Another way of extracting data from the Apple Watch, or in this case the suspected criminal, is to gather data from a cloud source such as iCloud. However, this acquisition method is not favorable because it requires law enforcement to jump through more hoops, obtain more warrants, or directly push the suspect to give them the password to the cloud account. On the other hand, if law enforcement is able to get that information from the suspect, they will find much more information than could be found on the Apple Watch alone, such as a comprehensive set of health information captured from the device over an extended period of time.

In general, Apple is known for being a very private and fairly locked-down, closed source company. However, as they continue to release innovative technologies that can capture more data, they will capture more data on their users for marketing and product development purposes. While most of the data captured is useful for end-users to see (health information, tracking information, text messages, etc.), the data captured by wearable devices can prove to be extremely useful in a forensics investigation, especially because criminals would likely forget to take the same precautionary measures they typically would on those devices. Lastly, the data that

wearable technology of today can and will capture is proving to be not only a lot more extensive than previous technology but also so extensive that data captured from a small wearable device such as the Apple Watch could exclusively be enough to provide incriminating evidence for a case.

References

Gillware. (2021, April 12). *Smartwatch forensics: Apple Watch Forensics: Gillware inc*. Gillware. Retrieved September 26, 2021, from https://www.gillware.com/flash-drive-data-recovery/smartwatch-forensics-apple-watch/.

Epifani, M. (2020, March 7). *Apple Watch Forensics 02: Analysis*. ElcomSoft blog. Retrieved September 26, 2021, from https://blog.elcomsoft.com/2019/06/apple-watch-forensics-02-analysis/.

Katalov, V. (2020, March 7). *Apple TV and Apple Watch Forensics 01: Acquisition*. ElcomSoft blog. Retrieved September 26, 2021, from https://blog.elcomsoft.com/2019/06/apple-tv-and-apple-watch-forensics-01-acquisition/.

Edwards, S., & Mahalik, H. (2015). Times 'a ticking to forensicate the Apple Watch! *Github*. Retrieved September 26, 2021, from https://github.com/mac4n6/Presentations/blob/master/Apple%20Watch%20-%20Times%20a'%20Tickin'/Apple_Watch_Times_a_Tickin.pdf.

Curry, D. (2021, August 16). *Apple Statistics (2021)*. Business of Apps. Retrieved September 26, 2021, from https://www.businessofapps.com/data/apple-statistics/.

Verizon. (n.d.). *A timeline: A brief history of Apple Watch*. verizonwireless.com. Retrieved September 26, 2021, from https://www.verizon.com/articles/brief-history-of-apple-watch/.

Arrows, K. (2021, July 22). *What are PLIST files and is it safe to delete them?* Appuals.com. Retrieved September 26, 2021, from https://appuals.com/what-are-plist-files-and-is-it-safe-to-delete-them/.