



Digital & Multimedia Sciences - 2017

C18 Paired Apple® Watch® Forensics

Yoshitaka Takase, MS, National Police Agency of Japan /Purdue University, 401 N Grant Street, West Lafayette, IN 47907*

After attending this presentation, attendees will be more familiar with paired iPhone® examinations. The implications for iPhone® examinations when paired with an Apple® Watch® will also be discussed.

This presentation will impact the forensic science community by providing information on the Apple® Watch® and paired iPhone® forensic artifacts.

An Apple® Watch® paired with an iPhone® provides not only precise time but also unique functions operating with installed applications and embedded equipment. There were some differences from conventional iPhone® examinations that could be recognized based on some research on an Apple® Watch® and the paired iPhone®. Factors changing the procedures are categorized into three groups, which are named influence, independence, and uniqueness for descriptive purposes. Influence is referred to as the pairing of an Apple® Watch® and an iPhone® and the influences the two devices have on each other. The interaction between them and the storage of Apple® Watch® data on the paired iPhone® are two examples. Independence is defined as separately processing and storing data on an Apple® Watch® and the paired iPhone®. Uniqueness encompasses Apple® Watch's® unique functions added to the paired iPhone®. These factors would bring new steps, new analyses, and new information, which is used for an iPhone® analysis to iPhone® examination processes. In the seizure phase, an Apple® Watch® should be isolated in order not to alter both data stored on the Apple® Watch® and the paired iPhone® because they communicate with each other via a wireless network. Also, the step to seize the Apple® Watch® needs to be added to the phase. In the collection phase, Apple® Watch® data should be extracted from the two devices; therefore, the step to extract the data from the Apple® Watch® needs to be conducted in this phase.

In this research, a manual extraction method (e.g., taking pictures or notes) was employed for the Apple® Watch®; also, an iTunes® backup method was used for the paired iPhone®. In the analysis and examination phase, the extracted data should be confirmed. The data from the Apple® Watch® were easily understood because the extracted data were pictures of applications displayed on the screen; however, there was extra work to figure out the data from the paired iPhone® because the backup contained a lot of files. Additionally, health data such as heart rates and active calories, which were sourced from the Apple® Watch®, could be analyzed by making more detailed charts than the charts displayed on the iPhone®. Also, information remaining on the Apple® Watch®, which has been deleted from the paired iPhone® could be applied to an analysis of the iPhone® in certain instances. The research concluded that pairing an Apple® Watch® and an iPhone® makes iPhone® examinations more complex and creates valuable data for forensic examiners.

Apple® Watch®, iPhone®, Wearable Device