C6 Connected Objects (Internet of Things [IoT]) as Crime Witnesses

Manon Fischer, MS, UNIL- Ecole des Sciences Criminelles, Lausanne, Vaud 1015, SWITZERLAND*

Learning Overview: After attending this presentation, attendees will be more familiar with traces from IoT devices in smart homes and understand how they can be used in an investigation context. The objectives of this presentation are to: (1) become more familiar with the different sources of traces available from IoT devices, such as traces on the smart phone, on the network, and on the cloud (available through personal data access); (2) demonstrate the investigative and forensic value of the traces in smart homes; and (3) illustrate how traces found during a simulated fire investigation helped with the reconstruction of the event.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by presenting the different sources of traces from IoT devices in smart homes and the value they have during an investigation. This presentation will also demonstrate how digital traces can be used in any case, such as fire investigation, to reconstruct real-world events.

Connected objects have invaded our daily lives. They are therefore more and more present in investigations of all kinds. Connected devices are witnesses that record and store data related to its environment. Since the connected devices have little memory, the data generated by these objects is stored elsewhere, remotely on the phones associated with them and in the cloud. Thus, traces generated during a fire, for example, are not necessarily destroyed when the connected device is destroyed or damaged.

A smart home was created for this study, and different scenarios were run. It was found that traces could be present on the network, on paired devices such as smart phones, and in the cloud. The scenarios reproduce, first, a normal activity and, secondly, activities taking place during a fire. Thus, it was necessary to study the behavior of the devices in case of electrical short circuit, network failure, and submission to heat.

Concerning the exploitation of network captures, it was possible to observe, on the one hand, with whom the objects communicated, and, on the other hand, the normal traffic generated by them. It was also possible to determine causes of disruption (electrical, network, or heat) using the presence or absence of traces, and when it happened. This information can guide the search and analysis of physical traces.

Traces from the cloud could be seen as latent traces in this context; traces are unknown to the investigator and have to be "revealed." Thus, this data is obtained using requests for personal data access (i.e., General Data Protection Regulation [GDPR] requests). It requires access to the user account but is quick and easy to obtain. The amount of data available depends on the device. It allows information on the user's interactions with connected devices and the environment to be obtained. Most of the available data is also time-stamped, which is useful for establishing a chronology.

In conclusion, systematically identifying the objects present on the scene and getting as many credentials about them as possible is recommended. In addition, it is necessary request access to personal data as soon as possible. This precious information will help in reconstructing digital and physical activities.

IoT, Network Analysis, Personal Data Access

*Presenting Author