C22 Smarthome Internet of Things (IoT) Traces: Forensic Potential and Challenges

Eoghan Casey, PhD, University of Lausanne, Lausanne, Vaud, SWITZERLAND; Joshua I. James, PhD, Hallym University, Korea, Gangwon 24252, SOUTH KOREA; Francesco Servida*, UNIL, Lausanne 1005, SWITZERLAND*

Learning Overview: After attending this presentation, attendees will better understand traces from IoT devices in smarthomes, how they can be useful in any investigation, and the challenges associated with evaluating these digital traces. This presentation has three objectives: (1) increase familiarity with traces from various IoT devices in a smarthome; (2) demonstrate how traces from IoT devices in a smarthome can be useful for investigative and forensic purposes; and (3) discuss evaluation challenges associated with traces from IoT devices in a smarthome.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by discussing traces from IoT devices in smarthomes, explaining the value of traces for any investigation, and the challenges associated with collection and evaluation of such traces when investigating criminal offenses.

IoT devices that provide home entertainment, comfort, convenience, and security can also contain vulnerabilities and generated traces. These digital traces can be useful for investigative and forensic purposes in any type of offense, including violent crime. At the same time, these traces can present evaluation challenges for forensic scientists and can create privacy risks for people in their homes.

Research and testing of various IoT devices was conducted in coordination with the Digital Forensic Research Workshop (DFRWS) IoT Forensic Challenges. These activities implemented various methods for obtaining traces from IoT devices, led to a deeper understanding of the traces generated by these devices, and led to tool development for specific types of traces. The simulated case scenarios focused on violent crime in order to connect digital traces with physical world offenses.

A combination of commercial, open-source, and bespoke methods were used to extract and analyze the traces. Traces were obtained from IoT devices themselves, from smart hubs, and from associated smart phone apps. Some information was obtained from network traffic and cloud-connected servers, but many transient or cloud traces were treated as out of scope in order to concentrate attention and activities on the physical location of a crime. Specialized forensic capabilities emerging from this work have been made available as open source.

Results of the coordinated research and testing are presented to highlight the potential value of such digital traces in any case, including violent crime investigation. In addition, the challenges associated with IoT traces are presented. Specifically, the challenges associated with preservation and analysis of these traces will be presented, and the difficulties in evaluation of forensic findings will be discussed. The need for future work is emphasized in order to keep pace with the rapid development of new smarthome IoT devices. Privacy and cybersecurity issues are raised in general terms to increase awareness of the risks associated with such devices.

Digital Forensic Science, Smarthome Forensic Analysis, IoT Trace