Chapter 1
IoT Forensic Science:
Principles, Processes, and Activities

Eoghan Casey
Université de Lausanne, Switzerland

Hannes Spichiger
Université de Lausanne, Switzerland

Elénore Ryser
Université de Lausanne, Switzerland

Francesco Servida
Université de Lausanne, Switzerland

David-Olivier Jaquet-Chiffelle
Université de Lausanne, Switzerland

ABSTRACT

IoT devices produce information that can be used in criminal investigations and cybersecurity incidents to make inferences about identities, locations, chronologies, and relationships between relevant entities. Before this information is relied upon to make critical decisions, its veracity must be assessed critically, and the link between virtual and physical worlds must be evaluated carefully. This chapter presents the forensic science principles needed to exploit the full potential of IoT traces, including uniqueness, exchange, provenance, integrity, reliability, repeatability, evaluating links between virtual and physical entities, and formally assessing alternative hypotheses. This chapter also discusses core forensic processes and activities, demonstrating their application to forensic analysis of IoT devices using practical examples. A typology of IoT traces is proposed and their usefulness during an investigation is discussed. Finally, an investigative scenario is presented to illustrate the opportunities and challenges of exploiting IoT devices and traces for investigative and forensic purposes.

DOI: 10.4018/978-1-7998-2444-2.ch001

INTRODUCTION

Rapid growth in the number, variety and complexity of IoT objects raises major challenges and opportunities for forensic science. These systems are becoming ubiquitous in public spaces, workplaces, schools, homes and other private areas, generating large volumes of data at high velocity in various formats. These digital traces can be analysed to make inferences about identities, locations, chronologies and relationships between relevant entities (Casey, Ribaux, & Roux, 2019). The purpose of forensic science in this context is to study digital traces in a systematic and coherent manner to address the questions of authentication, identification, classification, reconstruction and evaluation for a legal context (Pollitt, Casey, Jaquet-Chiffelle, & Gladyshev, 2018). The legal context can be the typical criminal, civil, and regulatory functions of the legal system, as well as its extensions such as human rights, employment disputes, natural disasters and security matters (e.g., critical infrastructure protection).

IoT devices can be targets, digital witnesses or instrumentalities of crimes and cyberattacks, creating new investigative opportunities, forensic challenges, security risks, legal issues, privacy risks and ethical conundrums. IoT devices can be exploited by a cyberattack, targeting the object itself or connected systems, including critical infrastructure, for various purposes (e.g., cyberstalking, fraud, espionage, botnets, DDOS) (Pour et al., 2019). Traditional criminals can manipulate or disable security systems supported by IoT devices such as door locks, alarms and cameras to facilitate burglary and other non-cyber offenses. Investigators of traditional crimes, including violent crimes, increasingly incorporate information produced by IoT devices to address questions about what happened around the time and place of an offense, and who was involved. However, to mitigate the risk of mistakes, the reliability of information from IoT devices must be assessed critically, and the link between virtual and physical worlds must be evaluated carefully.

The privacy risks associated with capturing information from IoT devices must also be mitigated. Some municipalities have become concerned about the use of technology to investigate crime, strictly controlling use of any *electronic device, system utilizing an electronic device, or similar technological tool used, designed, or primarily intended to collect audio, electronic, visual, location, thermal, olfactory, biometric, or similar information specifically associated with, or capable of being associated with, any individual or group* (Stop Secret Surveillance Ordinance, 2019).

The complexity of issues surrounding IoT devices as sources of evidence and instruments of invasion make it necessary to take a broader forensic science perspective, not just a technical one. Responding to this need, this work applies forensic science principles, processes and activities to IoT devices and traces. This chapter begins with an overview of IoT technology, prior work related to IoT forensics,