Chapter 15
Event Reconstruction:
A State of the Art

Yoan Chabot
University of Bourgogne, France & University College Dublin, Ireland

Tahar Kechadi
University College Dublin, Ireland

Aurélie Bertaux
University of Bourgogne, France

Christophe Nicolle
University of Bourgogne, France

ABSTRACT

Event reconstruction is one of the most important steps in digital forensic investigations. It allows investigators to have a clear view of the events that have occurred over a time period. Event reconstruction is a complex task that requires exploration of a large amount of events due to the pervasiveness of new technologies. Any evidence produced at the end of the investigative process must also meet the requirements of the courts, such as reproducibility, verifiability, validation, etc. After defining the most important concepts of event reconstruction, the authors present a survey of the challenges of this field and solutions proposed so far.

INTRODUCTION

Cybercrime and digital forensics have become increasingly commonplace in today's world. Crimes committed with the aid of or against digital systems are being reported almost daily. Internet fraud, cyber-bullying, cyber-terrorism, systems intrusion perpetrated against both individuals and corporations are costing businesses and governments billions in lost revenue and security updates (Anderson, et al., 2012). Due to all these issues, digital forensics has become an important research area in the last few years. Digital forensics is defined by (Palmer, 2001) as a set of methods based on proven scientific theories which aim to enable the reconstruction of past events related to an incident and the detection of criminal acts. To reach these objectives, each digital investigation is conducted according to a rigorous process (Palmer, 2001) starting with the identification of an incident and ending with the final decision of the court of justice. This process includes steps allowing to preserve the integrity of evidence, to seize sources of footprints from the crime scene, to examine these sources to find relevant information and finally to analyse this information to be able to make assumptions about the incident.

Several tools are available to help investigators during the first steps of this process. For example, EnCase or FTK can help investigative agents dur-

DOI: 10.4018/978-1-4666-6324-4.ch015

ing the collection and the examination of digital objects while preserving their integrity. However, these tools are limited regarding the analysis step, which allows to fully understand what happened during the incident. Collecting evidence and studying its properties is an important part of the investigative process. However, to extract acceptable evidence, it is also necessary to infer new knowledge such as the causes of the current state of the evidence (Carrier & Spafford, 2004). For example, a file illegally modified may be identified during the first steps of an investigation. Although the identification of such an object is interesting, only the analysis phase can help investigators to understand the causes of this modification. Among all the techniques used during the analysis phase, event reconstruction enables investigators to have a global overview of the events occurring before, during and after a given incident. The story produced as output of this process can answer many questions such as « What happened?" and "Why did these events took place?".

This chapter aims to present different aspects of the field of event reconstruction and outlines the various approaches proposed so far. After presenting several notions extensively used in this field (e.g. footprint, event, etc.), we reviewed challenges encountered during the conception of event reconstruction approaches. Then, the different approaches used to perform event reconstruction are introduced and assessed. For each of them, a description of the method used and a synthesis of strengths and limitations in relation to the challenges of the field are given. Finally, future directions for research are given.

DEFINITIONS

Event reconstruction is "the process of identifying the underlying conditions and reconstructing the sequence of events that led to a security incident" (Jeyaraman & Atallah, 2006). There are several types of event reconstruction depending on the nature of the incident. This chapter focuses on prosecutorial forensic analysis which is used to solve digital crime, and so, we explain the terminology we use.

First, the *crime scene* is a space where a crime or an incident takes place. (Carrier, Spafford, & others, 2003) defines a *physical crime scene* is defined as "a physical environment containing physical evidence related to an incident". The physical environment in which happen the incident is called the *primary physical crime scene*. Because of network connections for example, the crime scene can be extended to other places (e.g. if one of the protagonists has communicated with a remote party or download a file from a remote server, it can be necessary to seize the remote machines). The crime scene is not necessarily limited to a single building or environment and the subsequent scenes are called *secondary physical crime scene*. Then, a *digital crime scene* is defined as a component of a physical crime scene: "a virtual environment created by hardware and software and containing digital evidence related to an incident" (Carrier, Spafford, & others, 2003). A *physical crime scene* may contain several digital crime scene (a computer, a cell phone or other electronic device).

After the incident and the arrival of the officers in charge of the investigation, the crime scene becomes a protected space where the state of resources is preserved. After ensuring the protection of the crime scene, investigators start the *collection phase*. The purpose of this latter is to collect objects which carries footprints that can be relevant in respect to the objectives defined at the beginning of the investigation. The objects collected during an investigation carry digital footprints and may themselves contain many digital footprint sources (e.g. a computer may contain digital footprint sources such as Firefox logs, Apache logs, etc.). According to (Ribaux, 2013), a footprint (or a trace) is the sign of a past event. A footprint is the only available information to define the past events (e.g. a fingerprint indicates that an object