Chapter 1
Network Forensics:
Fundamentals

ABSTRACT

Network forensics investigations aim to uncover evidence about criminal or unauthorized activities facilitated by, or targeted to, a given networking technology. Understanding the fundamental investigative principles is equally important as understanding each of the modern networking technologies for every forensics scientist or practitioner. This chapter provides an overview of the network forensic fundamentals from a contemporary perspective, accenting the formalization of network investigation, various investigative techniques, and how the network forensics support the legal system.

INTRODUCTION

This chapter overviews the fundamentals of the network forensics practice. An updated network forensics definition is provided to reflect the proliferation of new networking solutions including mobile devices, smart objects, industrial controls systems, and cloud computing platforms. The standardized network forensics investigation process recommended by the International Standardization Organization (ISO) is presented throughout the chapter with supporting examples of mobile network investigations. In the same context, the network forensics techniques and their role in the legal system are also discussed. The chapter concludes with a brief review of the current mobile technology to set the accord for the remainder of this book.

DOI: 10.4018/978-1-5225-5855-2.ch001

DEFINITION OF NETWORK FORENSICS

Network forensics is a cross-discipline of digital forensics and communication networks. Digital forensics is the application of scientific methods to investigate evidence from digital sources about security incidents or criminal activities (Palmer, 2001; Ruan *et al.*, 2011). Communication networks refer to any infrastructure used for exchange of information in digital form between two or more network entities. In the early years, the network forensics focused on investigating Internet Protocol (IP) based networks for evidence in relation to malicious traffic packets or irregular traffic flows in violation of the networking policies and principles (Khan *et al.*, 2016).

As both the networks and the malicious behavior evolved, the forensics practice broadened to include mobile networks, cloud computing, Internet-of-Things (IoT), industrial control systems, and software-defined networks. The investigations in these environments follow the common network forensics investigation process with techniques, tools, and procedures tailored specifically for each of them. Modern network forensics thus refer to the *scientific methods for identification, collection, acquisition, and preservation of digital evidence from networking environments for further analysis, interpretation, and presentation in investigating security incidents and criminal activities*.

NETWORK FORENSICS INVESTIGATION PROCESS

Background

The formalization of network forensics is necessary to ensure the soundness and reliability of the investigative process and the veracity of evidence presented in court (Slay *et al.*, 2009). To demonstrate the suitability of the scientific methods for production of network evidence, various formal models have been proposed in the past (Marshall, 2011; Joshi and Pilli, 2016). The ISO recognized that the inconsistency between these models can greatly affect the quality, validity, and credibility of the digital evidence and devised accreditation through the set of interrelated standards depicted in Figure 1. These standards lay down the fundamental set of principles with guidance on how they can be applied in common scenarios. As such, the ISO/IEC SC27 standards are suitable for investigations in various networking environments to ensure the quality of the network forensics products.