Chapter 6
Mobile Network Forensics:
General Principles and Legal Aspects

ABSTRACT

The sensitive nature of mobile network forensics requires careful organization of the investigative processes and procedures to ensure legal compliance and adequate privacy protection. Investigations in mobile networking environments can be conducted for two main purposes: (1) to reconstruct criminal activities facilitated by a use of a mobile service and (2) to attribute malicious attacks targeting the normal operation of the mobile infrastructure. In both cases, investigators need to know the concepts introduced in the previous chapters to operationalize any mobile network related investigation. This chapter elaborates the legal framework, the general investigative principles, and evidence types characteristic for investigations in mobile network infrastructures.

INTRODUCTION

This chapter introduces the general principles of mobile network forensics together with the legal framework legislating investigations that aim to uncover mobile network evidence. Two main types of forensic investigations are covered, one concerning mobile network facilitated crime and other concerning mobile network targeted attacks. For the purpose of mobile facilitated crime reconstruction, the required architecture and necessary mechanisms for lawful interception and localization are described, together with the corresponding

DOI: 10.4018/978-1-5225-5855-2.ch006
Mobile Network Forensics

sources of mobile network evidence. For attributing mobile network targeted attacks, the utilization of the network performance measurement architecture for forensic purposes is explained in reference to known attacks against mobile networks. A review of the legal framework including the main interception laws is provided to assist with operationalization of the investigative principles and products elaborated throughout the chapter.

MOBILE NETWORK FORENSICS

Definition

Mobile network forensics is a cross-discipline of digital forensics and mobile 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). Mobile networks are a rich source of digital evidence and as such can help reconstruct any criminal activities facilitated by or targeted towards the network infrastructure. Formally, mobile network forensics refer to the scientific methods for identification, collection, acquisition, and preservation of digital evidence from mobile network infrastructures for further analysis, interpretation, and presentation in investigating security incidents and criminal activities. Mobile network forensics can also be denoted as cellular network forensics, referring to the cellular organization of the radio network subsystems.

Purpose and Investigative Types

The goal of the mobile network forensics is to investigate mobile network facilitated crimes and mobile network targeted attacks for the purpose of crime reconstruction or attack attribution, respectively. Mobile network facilitated crimes refer to any crimes carried out with the direct support of the network (e.g. perpetrators using mobile phones to communicate with each other) or the network is incidental to the crime (e.g. the network can provide historical data about perpetrators’ past movements or their subscription data). Mobile targeted attacks refer to any malicious or incidental activities aiming to disrupt the normal operation of the network (e.g. botnets of mobile users trying to saturate the network with large amount of bogus connection requests or traffic).
Opportunistic Software Deployment in Disconnected Mobile Ad Hoc Networks
www.igi-global.com/chapter/opportunistic-software-deployment-disconnected-mobile/65330?camid=4v1a

Multi-Layered Security Model for Hadoop Environment: Security Model for Hadoop
www.igi-global.com/article/multi-layered-security-model-for-hadoop-environment/214024?camid=4v1a