Digital Forensics 2.0
A Review on Social Networks Forensics

MohammadReza Keyvanpour1, Mohammad Moradi2, and Faranak Hasanzadeh3

1 Department of Computer Engineering, Alzahra University, Vanak, Tehran, Iran
   keyvanpour@alzahra.ac.ir
2 Faculty of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran
   Mhd.moradi@qiau.ac.ir
3 Department of Software Engineering and Artificial Intelligence, Science and Research Branch, Islamic Azad University, Qazvin, Iran
   F.hasanzadeh@qiau.ac.ir

Abstract. Nowadays, Social Networks (SNs) are penetrating into all areas of human life including relationships, shopping, education and so on and this growing expansion is inevitable. In addition to their invaluable benefits, due to the plethora of confidential private/corporate information in SNs, these places become the potential target for criminal/illegal activities such as identity theft, fraud, organized crimes and even terrorist attacks. To cope with such issues, it is useful to incorporate social network forensics (SNF) techniques for analyzing and surveying social interactions to detect, predict and prevent all forms of potential criminal activities. This chapter is organized in two main parts. First, SNs, their security and privacy issues are introduced and analyzed. Then, as a reference point for future studies in the field, forensics methods within SNs are explained and classified; then the related literature is reviewed.

1 Introduction

Nowadays Social Networks are an integral part of a large amount of people’s lives [1] in the broad range including students, athletes, artists and even politicians [2]. As is predictable, everybody uses SNs in his/ her own ways and interests. This fact shows flexibility and high-level potentiality of SNs, which make it adaptable to different situations and applications. In other words, declaring the situation of current web, social web – to bold the role and position of social media in general and social networks in particular- is the most appropriate and rational term. Due to the plethora of people, sensitive information and numerous SNs in different forms, these places turn into potential targets for attackers and become fertile fields for abusers. There are many threats to SNs which take advantages of their vulnerabilities and security breaches to attack privacy and exposure of confidential information. Fraud, espionage and scamming are only some of these criminal activities.

To alleviate such (mostly, privacy-related) issues, the most straightforward solution is to make the most of security mechanisms and configurations from SNs.
Moreover, as an influential factor, the ball is in the users’ court since they should take care of their private information. Frankly speaking, in practical terms, there is not any completely secure and invulnerable place on the web.

In addition to user-centered solutions, another supervisory way is to use (social networks) forensics techniques [3,4] and tools for analyzing and surveying social interactions to detect, analyze, predict and prevent all forms of potential criminal activities. Despite their total higher costs, they are generally efficient. Of course, in contrast to security and privacy preserving mechanisms and because of the nature of results, forensics methods are used by private sectors and organizations rather than regular users. Even, in most of the cases, there is a need for legal authorizations. In the field of SNF as a subset of digital forensics, due to specific features of SNs, in addition to standard forensics techniques, several context-specific ones have been also proposed that will be considered in detail in the rest of this chapter.

In this chapter, security issues of SNs will be considered with a focus on forensics tasks.

In fact, this chapter is divided into two main parts:

- **Security Issues of Social Networks**
  which includes a short background on social networks as the context, their different types and applications, negative aspects and security and privacy issues of SNs.

- **Social Networks Forensics**
  Including brief introduction of digital forensics, approaches towards social networks forensics and related topics and issues such as Social Networks Analysis (SNA) and Social Networks Mining (SNM). Moreover, a review on the literature of SNF will be performed.

The structure of this chapter is as follows: in Section 2, we take an overview on Social Networks, their history and different types. Section 3 introduces drawbacks and problems of Social Networking Sites. Security issues with Social Networking sites as well as their different aspects are explained in Section 4. Section 5 provides an introduction to Social Networks Forensics and its differences with Computer forensics as well as proposing a conceptual architecture of a typical SNF system. The literature of the topic is reviewed in Section 6.

2 **Overview of Social Networks**

In this section, as the context of SNF, we take a general overview on social networks - better to say, Social Networking Sites (SNSs) - and their different types, applications and related issues.

With the advent of the World Wide Web in the early 90s, contribution of digital media has been greatly changed due to facilitation of communications, access to resources, information sharing and so on. Despite its numerous benefits, there was a substantial drawback in the old web structure which was degree of collaboration. In fact, during those days, information was produced by owners and used by users. In this model, the only way through which users could participate was their comments