Journal of Network and Computer Applications 66 (2016) 214–235

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

# Network forensics: Review, taxonomy, and open challenges

Suleman Khan [a,b,*], Abdullah Gani [a,b,*], Ainuddin Wahid Abdul Wahab [b], Muhammad Shiraz [c], Iftikhar Ahmad [d]

[a] Centre for Mobile Cloud Computing Research (C4MCCR), University of Malaya, Kuala Lumpur, Malaysia
[b] Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia
[c] Department of Computer Science, Federal Urdu University of Arts, Science and Technology, Pakistan
[d] Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

ARTICLE INFO

*Article history:*
Received 8 January 2015
Received in revised form
20 January 2016
Accepted 7 March 2016
Available online 9 March 2016

*Keywords:*
Forensic
Investigation
Cybercrimes
Digital evidence
Intrusion detection

## ABSTRACT

In recent years, a number of network forensics techniques have been proposed to investigate the increasing number of cybercrimes. Network forensics techniques assist in tracking internal and external network attacks by focusing on inherent network vulnerabilities and communication mechanisms. However, investigation of cybercrime becomes more challenging when cyber criminals erase the traces in order to avoid detection. Therefore, network forensics techniques employ mechanisms to facilitate investigation by recording every single packet and event that is disseminated into the network. As a result, it allows identification of the origin of the attack through reconstruction of the recorded data. In the current literature, network forensics techniques are studied on the basis of forensic tools, process models and framework implementations. However, a comprehensive study of cybercrime investigation using network forensics frameworks along with a critical review of present network forensics techniques is lacking. In other words, our study is motivated by the diversity of digital evidence and the difficulty of addressing numerous attacks in the network using network forensics techniques. Therefore, this paper reviews the fundamental mechanism of network forensics techniques to determine how network attacks are identified in the network. Through an extensive review of related literature, a thematic taxonomy is proposed for the classification of current network forensics techniques based on its implementation as well as target data sets involved in the conducting of forensic investigations. The critical aspects and significant features of the current network forensics techniques are investigated using qualitative analysis technique. We derive significant parameters from the literature for discussing the similarities and differences in existing network forensics techniques. The parameters include framework nature, mechanism, target dataset, target instance, forensic processing, time of investigation, execution definition, and objective function. Finally, open research challenges are discussed in network forensics to assist researchers in selecting the appropriate domains for further research and obtain ideas for exploring optimal techniques for investigating cyber-crimes.

## Contents

[*] Corresponding authors at: Centre for Mobile Cloud Computing Research (C4MCCR), University of Malaya, Kuala Lumpur, Malaysia.
*E-mail addresses:* suleman@siswa.um.edu.my (S. Khan), abdullah@um.edu.my (A. Gani).

http://dx.doi.org/10.1016/j.jnca.2016.03.005
1084-8045/© 2016 Elsevier Ltd. All rights reserved.

## 1. Introduction

The advent of network forensics envisioned several investigation methods for network security breaches and vulnerabilities. These methods rely heavily on identifying, capturing, discovering, and analyzing network traffic encompassing network devices as well as infrastructure (Nelson et al., 2010). To enable network forensics in the presence of network security suspects, the basic precondition is the ability of an investigator to discover the main objective of the investigation (Raftopoulos and Dimitropoulos, 2013). Usually, there are various types of investigation, i.e. undertake a criminal investigation (Mosa and Jantan, 2013), archive contexture for an internal corporate investigation (Perry, 2006), and retort to a particular network incident (Bejtlich, 2013). Each of these investigations has different intentions and procedures; however, the common goal is to investigate network traffic which is collected during different events at the time of network susceptibilities. These investigations correspond to network attacks (Hoque et al., 2014) and its consequence on the network. In addition, network forensics consents to explore digital evidence in the network traffic after the occurrence of the suspected event (Cusack and Alqahtani, 2013). It allows to reform the complete pattern of network attacks that occurred initially in the network. Traditionally, network forensics reconstructs network attack by capturing network traffic at one device and transmits it to other devices for analysis (Chen et al., 2013a; Ibrahim et al., 2012; Jeong and Lee, 2013; Ren, 2004; Wang et al., 2007). However, it is found that transmitting huge amount of data from one device to another overloads the available communication channel and results in time delays (Ibrahim et al., 2012; Kim and Kim, 2011). Moreover, it affects network forensics performance in real-time situation by resulting in poor incident response. It implies that refined methods are required for analyzing network traffic that can satisfy various requirements of network forensics and network security.

Over the years, an extensive range of network forensics techniques (NFT) has been proposed with distinct investigation approaches (Chen et al., 2013a; Fan and Wang, 2010; Fen et al., 2012b; Lin et al., 2010; Ren and Jin, 2005). Such approaches have the sole goal of extracting legal evidence from network security devices and network communication channels that are connected to such network devices. Legal evidence is analyzed using NFT to identify the origin of the attack. For instance, NFT in Jeong and Lee (2013) shows that by capturing network traffic at router is analyzed to discover the origin of the attack which exposes an intruder. Despite extensive research on NFT, only a single study surveyed network forensics Pilli et al. (2010). The study in Pilli et al. (2010) presents outline on network forensics tools, process model, and framework implementation. A comprehensive study of cybercrime investigation using network forensics frameworks along with a critical review of the current network forensics techniques is lacking. However, no such study has been presented including (Pilli et al., 2010), that focuses on the implementation as well as target datasets of NFT with further illustration on the critical aspect of frameworks for NFT.

This study is conducted in view of the diversity of digital evidence and the difficulty of addressing numerous attacks in the network through NFTs. This paper focuses on NFTs with three distinct objectives: (1) accessibility to network artifacts and infrastructure, (2) allows adequate evidence against intruder, and (3) using NFT as a means to convey information regarding malicious attacks with less false negative results. Two basic reasons motivate this selection: (1) all of these NFT aim to provide digital evidence that require intruders to put in more efforts and time to attack, and (2) this selection narrows down the scope and consents for a comprehensive study of the area. The objective of this study is to provide researchers with a comprehensive insight about the state-of-the-art and open challenges to NFT. This study would be even an important contribution to legislators and security agency committees relating to the formulation of standard legal frameworks.

This paper reviews the fundamental mechanics of NFTs, to determine how network attacks are identified in the network. With reference to an extensive review of related literature, a thematic taxonomy is proposed for the classification of current NFTs based on its implementation as well as target data sets involved in the conducting of forensic investigations. A qualitative analysis technique is presented to explore the critical and significant aspects of existing NFTs. We derive parameters including framework nature, mechanism, target dataset, target instance, forensic processing, time of investigation, execution definition, and objective function for discussing the similarities and differences in current NFTs. Finally, open research challenges are discussed in network forensics to assist researchers in selecting the appropriate domains for further research and obtain ideas for exploring optimal techniques for investigating cybercrimes.

The followings are the contribution of the paper: (a) Classification of the frameworks for NFT on the basis of thematic taxonomy. (b) Analysis of current NFT by discussing the