Journal of Forensic Sciences And Criminal Investigation
ISSN: 2476-1311

Juniper Publishers key to the Researchers

Review Article
Volume 13 Issue 1 - November 2019
DOI: 10.19080/JFSCI.2019.13.555853

J Forensic Sci & Criminal Inves

Network Forensics: Concepts and Challenges

Antonio Cortés Castillo*

Departamento de Informática, Universidad de Panamá, Panamá

Submission: October 01, 2019; **Published:** November 05, 2019

***Corresponding author:** Antonio Cortés Castillo, Departamento de Informática, Universidad de Panamá, Panamá

Abstract

The forensic network is a branch of the typical digital forensic analysis that is responsible for monitoring, capturing, recording and analyzing data traffic on the network. However, implies the use of scientifically proven techniques to collect and analyze network packages and events for research purposes. Forensic network analysis is an extension of the network security model that traditionally focuses on preventive analysis and detection of network attacks. Similarly, this current model allows analyzing malicious behavior in networks. In addition, it allows organizations to carry out investigations related to attacks on the corporate network from an internal and external environment. In this article, several aspects of the forensic network are reviewed, similarly, related technologies and their limitations. Together, the challenges in shaping a forensic network infrastructure are highlighted.

Keywords: Network Forensics; Network Security; Computer forensics; Computer security

Abbreviations: IDPS: Intrusion Detection and Prevention Systems; IDIP: Integrated Digital Research Process; IDS: Intrusion Detection System; USB: Universal Serial Bus; SSD: Solid State Drive

Introduction

Digital forensic science [1] has evolved as a science related to the recovery of evidence located in a computer system, storage in devices whether these are permanent or erasable, electronic documents such as emails or images and a sequence of data packets transmitted through a computer network. Unlike other areas of digital forensic science, network investigations are treated as volatile and dynamic (live) information. This allows the network traffic to be transmitted while remaining unavailable, which makes the forensic network a dynamic and proactive network. Therefore, in a digital forensic process it is common to focus on extracting already stored data. However, the forensic network is a branch of digital forensic science that involves monitoring and analyzing network traffic, in order to gather information, legal evidence or intruder detection. A relevant aspect of forensic medicine is related to the processes that are carried out in «real time» or «after the event». An organized approach is the key to successful research. With the continued growth and expansion of the Internet, cyber -attacks and crimes occur every day [2], which allows the intruder's skills to be increased using malicious software, for example, malware. This raises the fact that you will be attacked at any time, but I don't know when. Hence, the emergence of traditional tools used in investigations, such as firewalls and intrusion detection and prevention systems (IDPS) but are not enough since they cannot provide all the required evidence or data [3]. However, when it comes to network security, organizations generally use tools to address security from two main perspectives: Prevention and Detection. Investigating attacks is a difficult task. Prevention systems include firewalls and access control mechanisms. Similarly, examples of detection include intrusion detection systems and antivirus. However, the tools used prevent numerous attacks, but despite the preventive measures implemented in organizations, there will always be attacks that cannot be identified and recognized. The forensic network is recommended as a complement to the network security model.

In the context, the network forensic refers to a dedicated research infrastructure that allows the collection and analysis of network packages and events for research purposes. It is proposed as a complement to the network security model [4,5]. In the forensic network the monitoring and analysis of the traffic of the computer network is carried out, both locally and at the WAN level, which allows the collection of information, as well as the collection of evidence or the detection of intruders [6]. In data traffic, data packets are intercepted for later storage for analysis or real-time filtering. The forensic network generally has two uses. First, security identification includes verifying a

system and recognizing interruptions and second, application identification, where the analysis of captured network traffic can include tasks such as assembling exchanged files, searching keywords and analyzing correspondence between humans, such as emails, chat sessions, messaging at WhatsApp's level, social networks like Facebook.

Materials and Methods

Concept of network forensic

The term network forensic was previously used in a few contexts without an official definition [7]. In the forensic network it deals with data located through the network connection, between the various interconnected nodes, mainly data traffic entering and leaving these nodes. The forensic network analyzes the data from the data traffic that is generated through the respective firewalls or IDS or on network devices such as routers. The goal is to track the source of attack so that cyber criminals are prosecuted. The forensic network is defined as "The use of scientifically proven techniques to collect, merge, identify, examine, correlate, analyze and document digital evidence from multiple sources of digital processing and active processing in order to discover facts related to the planned intention of unauthorized persons oriented to carry out activities aimed at interrupting, corrupting or compromising system components, as well as providing information to assist in the response or recovery of these activities [8]". Network research involves the reform and analysis of computer network data associated with unauthorized access. Its purpose is to allow specialists to reason about the circumstances of the activity being investigated and to present evidence before the court of law. The network forensic is characterized by detecting, recognizing and assigning responsibilities for attacks. against our data network infrastructures. In turn, it defines the use of safety devices and their review data to guarantee the obtaining of evidence. Similarly, it determines the use of networks for the collection of static information during the investigation. In general, investigations in networks forensic will use events, allowing investigations and schemes to be recorded to determine the following:

a) Who: is to blame for the action?

b) What: the attacker has done.

c) When: the next event will happen.

d) Where: the location of the node where the attack

e) occurred is identified.

f) Why: the crime occurred, what were your reasons for guilt.

g) How: was the source used or vulnerabilities found.

With numerous illegal activities, including the network, this type of investigation is being carried out in a large number and structure of essential component computers in forensic networks.

Model

In theory, digital forensic and, therefore, network forensic analysis are not protection products. It is not supposed to replace firewalls and intruder detection systems. However, it is a complex process in which methodologies, tools and human intelligence are combined for research purposes. In the literature, few models have been proposed to model the digital forensic process [4,5,9-11]. There is no consensus on which model best or even correctly represents the process. However, the proposed models share a common basis when fine details are ignored. They are based on standard research models that are applied in real-life crimes. The Integrated Digital Research Process (IDIP) is a representative model of the digital forensic process [8]. This is made up of a series of levels that are organized into five groups as seen in Figure 1 The following is a brief description of these groups:

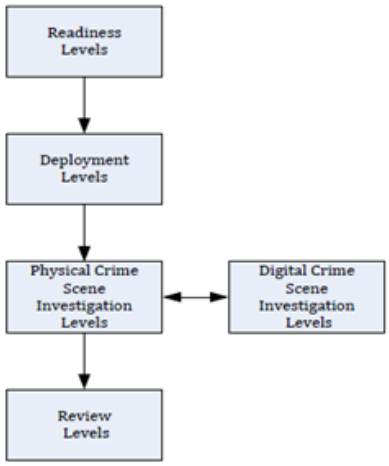

Figure 1: The Integrated Digital Research Process (IDIP).

How to cite this article: Antonio Cortés Castillo. Network Forensics: Concepts and Challenges. J Forensic Sci & Criminal Inves. 2019; 13(1): 555853. DOI: 10.19080/JFSCI.2019.13.555853

Readiness levels

It ensures that personnel and infrastructure can support an investigation when an incident occurs.

Deployment levels

It provides a mechanism to detect an incident and confirm it.

Physical crime scene investigation levels

In this phase the physical evidence is collected and analyzed and the scenes that took place during the incident are reconstructed.

Digital scene investigation levels

The digital devices that were obtained from the levels of physical research are analyzed.

Review levels

All research is reviewed and those areas to be improved are identified.

State of the Art

The forensic network is currently a manual and slow process [12]. It is usually carried out by experienced system administrators. A typical investigation begins with the analysis of several types of records. In a typical network configuration, records can be in several places. For example, a network is usually equipped with an audit facility, such as Syslogd in Unix. In addition, applications such as web servers and network devices such as routers and firewalls maintain their own records. There are several tools and scripts (source code) that are generally used for research. For example, in a Unix environment, a researcher can make use of free utilities such as tcp dump [13], grep, strings, etc. Some researchers use commercial tools known as network forensic analysis tools [14-16]. The architectures of these commercial tools are not revealed. However, they provide similar features to those free utilities. Although they are easier to use and versatile. Besides, forensic network analysis is generally a manual and brute force process, which is usually slow and error prone. In this same direction, the records are not intended for a thorough investigation, since these may lack enough details or, conversely, have many unrelated details. They also come in different formats and incompatible levels of abstraction.

Related Technologies

In this section, related technologies are reviewed showing their connection to network forensics and their limitations.

Intrusion detection systems

An intrusion detection system (IDS) is made up of a system whose purpose is to detect computer and network attacks [17,18]. In turn, it monitors computer resources, a single node or a complete network, and generates alerts when an attack is detected. IDSs are implemented based on the nodes that exist in the computer network or the same network architecture. In addition, they use two main approaches to detect attacks:

Signature based: In this approach, detection is achieved by comparing a database of known attacks.

Based on anomalies: In this approach, an IDS generates a "normal" activity model of a system and then alerts when a deviation is detected.

In the context of the forensic network, an IDS is a valuable addition to a forensic network system. It can play the role of a sensor which triggers the forensic process. In addition, the alerts generated constitute an important source of information that can be collected and analyzed later. These alerts also help the analysis of data collected from other sources. There are several limitations related to the use of IDS in the field of forensic network:

Reliability in detection

When relying on the output of an IDS, there are several concerns. First, an IDS suffers from false alarms, such as a false positive that refers to the case when an IDS generates an alert for a non-existent attack, while a false negative refers to the case when an IDS fails in a real attack. The second concern is related to network-based IDS. They can be a target for known classes of attacks, for example, evasion and insertion attacks [19].

Data details

In general, the production of IDS lacks enough details for serious investigation. Usually, the output is a one-line text alert.

Honeypots

A honeypot refers to a set of services, a complete operating system or even a complete network that is designed to attract and contain intruders [20,21]. Although honeypots are destined to be compromised, they are a tight seal that is well controlled and monitored. Essentially, all honeypots share the same concept. It has no production value or authorized activity. However, any attempt to interact with them is probably malicious. In addition to containing and studying attacks, it can also be configured to divert attention from real targets [22]. In the context of the forensic network and from an investigative perspective, a honeypot is an ideal tool to closely study attackers and capture their tools, keystrokes, etc. Few studies have been proposed to adopt honeypots for forensic purposes [23-24]. A notable example is the Honeynet Project, a voluntary research organization dedicated to studying the tools, tactics and motives of the attackers [25]. In the context of constraints and from a legal point of view, honeypots can be problematic for two reasons. First, a honeypot has no value. It is configured only to be compromised and attacked. Therefore, compromising it does not incur any harm. In turn, it is not possible to legally claim any damage. Second, honeypots can be considered as a boundary between keeping attackers out of a network and inviting them [25].

How to cite this article: Antonio Cortés Castillo. Network Forensics: Concepts and Challenges. J Forensic Sci & Criminal Inves. 2019; 13(1): 555853. DOI: 10.19080/JFSCI.2019.13.555853

Computer Forensics

The computer forensic is the oldest member of the family of digital forensics. Traditionally, it refers to the forensic analysis of independent computers located at the crime scene [24]. It involves analyzing data storage devices, such as hard drives. Usually, a researcher uses specialized software to recover deleted files, encryption keys, passwords, emails, etc. Forensic computing has evolved over time following the standard methodologies used by the police to investigate real-life crimes. However, the computer itself is not the victim of an attack, it is a tool used by a criminal. The forensic process follows well defined procedures to preserve, identify, extract, document and interpret the data recovered on the seized computer. In general, forensic computing is not limited to personal computers. It also refers to the investigation of other digital devices that have some type of data storage medium, for example, cell phones, PDAs, digital cameras, among others. Similarly, computers can be found in crime scenes or with suspects. In the context of the forensic network, investigating involves using computer forensic techniques to investigate computers as if they were not networked. Otherwise, a networked computer can be isolated to start the respective analysis of it independently. Consequently, computer science and computer forensics network complement each other. With respect to limitations, forensic computing is only used to investigate independent computers. In addition, it lacks in terms of networked computer research. It does not address the problems that arise as a result of distributed data sources but centralized ones. Such problems include data correlation, propagation of attacks, etc. In turn, forensic computing deals exclusively with persistent data stored on a hard drive or other media, for example, USB, SSD, etc. However, in a network environment, it is necessary to deal with volatile data such as data traffic on the network. Consequently, forensic network analysis requires live data collection and analysis.

Challenges

A challenge in the forensic analysis of the network is to first ensure that the network is adequate to the forensic needs. For a successful investigation of the network, it must be equipped with an infrastructure that allows the research to be fully supported [4,5,9,10,19]. The infrastructure must ensure that there is the necessary data for a full investigation. Designing a network forensic infrastructure is a complex task due to the many possibilities that exist in how the design is done in the various spaces. The following is a brief description of some of these challenges:

Data sources

A typical network is made up of several data sources that include unprocessed network packets and records of network devices and services. Although it is desirable to collect data from all sources, this option is not always feasible, especially in those ecosystems consisting of large network infrastructure. Therefore, an important decision is to select a subset of data sources that provide good network coverage and make the collection processes practical [26].

Granularity in the data

A problem related to the selection of data sources is to decide how many details should be maintained. For example, when packets are collected on the network, full packages, packet headers, connection information, for example, IP addresses, port numbers, etc. can be collected. Similarly, maintaining extensive data details is not practical in large and complex networks [27].

Data integrity

It is essential to ensure the integrity of the data collected. The result of the forensic process may be adversely affected if the data collected is accidentally altered. However, measures must be implemented to ensure data integrity during and after data collection and analysis.

Data as legal evidence

The use of data collected internally within an organization is quite different from how the data is presented in a court of law. In the latter case, the data collected must pass written legal procedures to qualify as evidence in a court of law. The data must go through an admissibility test and a selection process by the court [20,21].

Privacy issues

The data collected is expected to include confidential information, such as emails and files. However, proper handling of this data is crucial. The data must be protected by access control measures, so only authorized personnel have access [28-30].

Data analysis

An important challenge is the analysis of the data collected to produce useful information that can be used in a decision-making process. Such an analysis process is in many ways challenging due to the complexity of a typical network environment and the amount and diversity of data involved. Innovative tools are needed to help researchers analyze the data. These tools allow the use of field tools such as data mining [22] and information visualization [23].

Conclusion

Today, organizations use various tools to protect their computer network. While these tools overcome many attacks, new attacks still evade prevention tools without being detected. In these circumstances, starting with investigations of attacks on the network is a complicated and difficult task. In the literature on computer security, it has been proposed that forensic network analysis introduce investigative capabilities into current networks. This refers to a research infrastructure that allows the collection and analysis of network packages and events for research purposes. In this article, various aspects of the network forensic were reviewed, as well as related technologies and their

How to cite this article: Antonio Cortés Castillo. Network Forensics: Concepts and Challenges. J Forensic Sci & Criminal Inves. 2019; 13(1): 555853. DOI: 10.19080/JFSCI.2019.13.555853

limitations. In addition, the challenges in the deployment of the forensic infrastructure of the network were highlighted.

References

1. Anstee D (2012) Worldwide Infrastructure Security Report, Arbor Networks, p. 4.
2. Lazzez A (2013) A Survey about Network Forensics Tools. International Journal of Computer and Information Technology 2(1): 74-81.
3. Q Al Mousa, ZA Al Mousa (2013) Honeypots Aiding Network Forensics: Challenges and Notins. Journal of Communication 8(11): 700-707.
4. Palmer G (2001) A road map for digital forensic research, in Digital Forensic Research Workshop, Utica, New York, USA.
5. (2001) Electronic Crime Scene Investigation: A Guide for First Responders, US Department of Justice: National Institute of Justice.
6. Mate MH, SR Kapse SR (2015) Network Forensic Tool Concept and Architecture. Fifth International Conference on Communication Systems and Network Technologies, Gwalior, Madhya Pradesh, India, pp. 711-713.
7. Ranum M (1997) Network forensics: Network traffic monitoring. Network Flight Recorder.
8. Almulhem A (2009) Network Forensics: Notions and Challenges. IEEE.
9. Beebe N, Clark JG (2005) A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation 2(2): 147-167.
10. Baryamureeba V, Tushabe, F (2004) The enhanced digital investigation process model. in Digital Forensic Research Workshop, Utica, New York, USA.
11. Carrier B, Spafford EH (2003) Getting physical with the digital investigation process. International Journal of Digital Evidence 2(2).
12. Fennelly C (2000) Analysis: The forensics of internet security. Sun World.
13. Jacobson V, Leres C, Mc Canne S (2007) Packet capture library.
14. King N, E Weiss E (2002) Analyze this! Information Security Magazine.
15. Enterprise N (2007) Net detector: Proactive security surveillance solution.
16. Enterprises S (2007) Net intercept: A network analysis and visibility tool.
17. Lunt T (1993) Detecting intruders in computer systems. in 1993 Conference on Audit and Computer Technology.
18. Roesch M, Green C (2003) Snort User Manual.
19. Ptacek T, Newsham T (1998) Insertion, evasion, and denial of service: Eluding network intrusion detection." Secure Networks, Inc.
20. Kruse JHWG (2001) Computer Forensics: Incident Response Essentials. Addison Wesley, New York, USA.
21. Scottberg B, Yurcik W, Doss D (2002) Internet honeypots: Protection or entrapment?" in Proceedings of the IEEE International Symposium on Technology and Society (ISTAS).
22. Almulhem A, Traore I (2005) Experience with engineering a network forensics system. Lecture Notes in Computer Science 3391: 62-71.
23. Spitzner L (2007) The honeynet project.
24. Tan PNSteinbach, M, Kumar V (2005), Introduction to Data Mining. Addison-Wesley.
25. Sommer P (1999) Intrusion detection systems as evidence. Computer Networks, p. 31.
26. Brezinski D, Killalea T (2002) Guidelines for evidence collection and archiving. RFC 3227, BCP 55.
27. Marty R., (2008), Applied Security Visualization. Addison Wesley, New York, USA.
28. Takemori K, Rikitake K, Miyake Y, Nakao K (2003) Intrusion trap system: An efficient platform for gathering intrusion-related information, in 10th International Conference on Telecommunications 1: 614-619.
29. Yasinsac A, Manzano Y (2002) Honeytraps, a network forensic tool, in Sixth Multi-Conference on Systemics, Cybernetics and Informatics.
30. Redmon B (2002) Maintaining forensic evidence for law enforcement agencies from a federation of decoy networks: An extended abstract. Mitretek Systems.

DOI: 10.19080/JFSCI.2019.12.555853

How to cite this article: Antonio Cortés Castillo. Network Forensics: Concepts and Challenges. J Forensic Sci & Criminal Inves. 2019; 13(1): 555853. DOI: 10.19080/JFSCI.2019.13.555853