# NetworkForensic Application in General Cases

Akhyar Lubis[1], Andysah Putera Utama Siahaan[2]
*Faculty of Computer Science*
*Universitas Pembangunan Panca Budi*
*Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing, 20122, Medan, Sumatera Utara, Indonesia*

***Abstract:****The common cases that often occur on a computer network is a weak point of computer security on computer networks. Network Forensic is a process of analyzing activity, recording, or even to identify the network to find digital evidence from a computer crime. Since the existence of the Internet as a global communication tool, it is a crime that often occurs gap. Internet containing the network forensics and lawful interception are important tasks for many organizations including small medium business, enterprises, banking and finance industry. This archiving and restoration of internet data can be used for legal evidence in case of disagreement. Government and intelligence agencies use technology to protect and defend national security. In general, computer forensics is simply the application of computer investigation and analysis techniques to determine the legal evidence that may be. There are several ways to find a crime on a computer network. The use of several applications supported are to improve the success of network forensic processes in the common cases.*

***Keywords:*** *Network Forensic, Digital Evidence, Threat*

## I. Introduction

Internet connectivity continues to link million of devices through the network connection. It makes them very vulnerable to be attacked [2]. Network forensics is an activity capture, record and analyze events on the network to find the source of security attacks or other activities issues. The strength of forensics is to allow analysis and regain facts and events of the environment, because the facts may be hidden. Different from forensics in general, computer forensics is the activity of collecting and analyzing data from various computer resources. Logs from the computer is an antivirus, database or application used [7].

Network forensics is part of digital forensics, where the evidence was captured from the network and interpreted based on knowledge of network attacks. It aims to find the attacker and reconstruct action attack attacker through analysis of evidence tampering. SQL injection occurs when an attacker could insert a series of SQL statements to query by manipulating the input data to the application. While on, SQL Injection is an attack targeting methodology of data in the database through a firewall that protects the data.

Network forensics comes from network security and intrusion detection. Network forensics related to the change of data from millisecond to millisecond. Investigation of cyber attack or intrusion is an investigation of network forensics. The main challenge facing of network forensics is how to retain evidence later used in court [6].

Combating internet crime has become a major portion of the law enforcement agencies and intelligence services, both nationally and internationally, not least business practitioners, the customer, to the end-user. Internet crime begins with the hosts and exploits computer networks so that the swindlers and the intruders came across networks, especially networks based on TCP / IP [4][5].

## II. Related Works

Meghanathan discusses various tools and techniques available to conduct network forensics. Among the tools discussed are eMailTrackerPro to identify the physical location of the sender's email, Web Historian to know how long each file upload and download of websites visited, packet sniffers such as Ethereal to capture and analyze the data exchange between different computers on the network. The study also reviews the different search techniques to mark the IP packets in helping a forensic investigator to identify the sources of attacks and also about the use of Honeypots and Honeynets. It can be concluded to detect all kinds of attacks and perform forensic analysis of a comprehensive; one must deploy and analyze the effectiveness of commercial tools and explore the tools and techniques for network forensics [3].

Ruchandani has done experiments with network forensics necessary traffic capture packets on the network, analyzing its characteristics, and trying to figure out a dangerous activity in helping to identify the source of activity as the damage done to the network using tools TCP-dump, ethereal, and n-map.It was concluded that the TCP-dump, ethereal, and n-map is very powerful to help capture and analyze network packets including packet sniffing and port scanning [1].

DOI: 10.9790/0661-1806044144

Furthermore, the study discusses the ForNet, to monitor, collect and retain data to support forensic network on the internet. ForNet is different from the logger; it produces a compact summary of the raw data network known as the synopsis.

Synopsis capture enough information to conduct an autopsy effective. ForNet is also implementing a distributed collection strategy.The study discusses the system of forensic logging of Network Processor (NP) to gather evidence, track suspicious behavior and evaluate the level of damage to the machine being attacked. Forensics as a science related to the new security capture, analysis, and reconstruction aims to make accurate evidence.

The main task of the forensic analysis and reconstruction. Interest logging system forensics is a system that monitors server activity to the kernel of the server operating system. It updates the user details collected from the server to the Network Processor (NP) and sent to the server forensics (machine log) in which an operating system to ensure access control, and the availability of base the data in response to queries from the log file is saved to the server forensics.

## III. Proposed Work

### *A. Methodology*

There are several steps to do a forensic process. It is combined to retrieve the conclusion or result. The process is done to know what has happened to the network. The phase are divided into four steps as shown in Figure 1. There are:

**1. Collection.**

At this stage it is done researching and looking for evidence, the introduction of the evidence of an intrusion, and evidence collection.Snort IDS systems are used to detect attacks. In Snort there is a rule that extracts characteristics of the packet over the network, so that if any suspicious packages and by the rules and sending alert messages and save them as a log.

**2. Preservation.**

At this stage, the search for hidden information and disclose relevant documentation. Examinations performed on the log file that has been taken using IDS Snort. After the log is stored as an alert, then log researched and examined. For example checking packet sequence.

**3. Analysis.**

Aesthetically results of the assays for evidentiary value in the case at hand. This stage is used to answer forensic questions that attack what happened, IP who carried out the attack, when the attack took place, where the attack took place, how the attack could happen, and why it happened.

**4. Presentation.**

Writing a report on the inspection process and the data obtained from all of the investigation. To create a report about the attack, which occurred on the network from the analysis of the evidence log, and once that is done the reconstruction of the data stream from the incident. Certainly not damage the existing log.

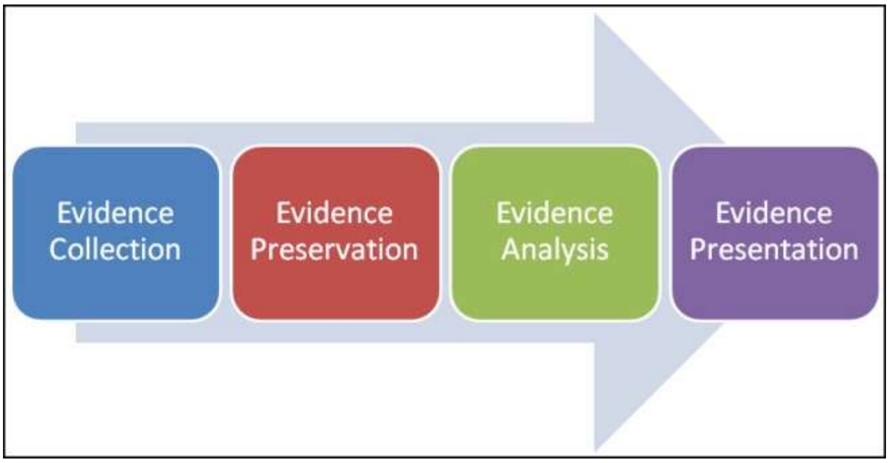

**Fig. 1** Network Forensic Phase

### *B. Network Tools*

Network forensics tool is the application used for the forensic experts who used to do things related to forensic such as monitoring and audit on the network. Toolkits for forensic testing make it possible to collect and analyze data such as E-Detective, NetFlow v5 / 9, netcat, NetDetector, TCP dump, Wireshark / Ethereal, Argus, NFR, TCPWrapper, sniffer, nstat, and tripwire. In the classification for tools that are divided into two, GUI and Command Line.

**GUI-based network forensics:**

a. Wireshark / ethereal

It is an analyzer and monitoring network that is popular. The features in wireshark are:

- can check hundreds of protocols in depth
- be able to catch a direct and analyzed offline
- multi-platform, can run on Windows, Linux, Mac OS X, Solaris, FreeBSD, NetBSD, and others.
- network data that has been captured can be displayed via the GUI or via the TTY-mode on utility tshark.
- can filter the view by many filter options.
- can read and store different formats.

**b. Netcat**

It is a utility tool that is used for a wide range of issues related to TCP or UDP protocol. That can open a TCP connection, send UDP port to listen on TCP and UDP ports, port scanning, and by IPV4 and IPV6.Netcat is usually used by the hacker or hackers to connect back to the target system so that hackers gain root access through the port that has been set by the hacker.

**c. E-Detective**

It is a system that does the interception of the Internet in real-time, monitoring and forensics systems that capture, code reading, and restore some types of Internet traffic.These systems are typically used in corporate Internet and monitor behavior, audit, storage of records, forensic analysis, and investigations. E-Detective can read the code, reassembly, and recover various types of Applications Internet and to services for example e-mail, Webmail, Instant Messaging, File Transfer, Online Games, Telnet, HTTP, VOIP, and others.

**Console-based network forensics:**

**a. TCP dump**

It is often used as a packet sniffer is used for UNIX-like OS, such as Linux, BSD, and others. Tcpdump produce a description of the content of network packets that match the boolean expression can be determined by the user.

**b. ARP**

Address Resolution Protocol ARP is a protocol within the TCP / IP Protocol Suite responsible in conducting IP address resolution into a Media Access Control address (MAC address).ARP is a protocol that serves IP address mapped into a MAC address. He is the link between the data link layer and IP layer in TCP / IP. All Ethernet-based communication uses this ARP protocol. Essentially any computer or device that will communicate will surely make transactions or exchange of related information between IP and MAC address. Each transaction will be stored in the cache of your OS. Can be viewed using the arp command (either in Windows or Linux).

**c. Ifconfig**

Ifconfig or Interface Configuration is a command on Linux which is used to configure the network interface. Ifconfig widely used to initialize the network interface and to enable or disable the interface. Used to view your IP address and your Mac.

**d. Ping**

Ping is a utility that is used to check the connectivity of the network through a protocol Transmission Control Protocol / Internet Protocol (TCP / IP) by sending a package of Internet Control Message Protocol (ICMP) to the IP address to be tested connectivity. Ping is used to sending packets to investigate the remote machine.

**e. Snoop**

Snoop is used to capture packets from the network and display its contents (Solaris).

**f. Gnetcast – GNU**

It is to rewrite the netcat.

**g. Network Mapper**

It is an application or a tool that serves to conduct port scanning. Nmap made by Gordon Lyon, known by the name of Fyodor Vaskovich. This application is used to re-audit existing network. By using this tool, we can see a host of active, open ports, operating system used, and other scanning feature-feature. Nmap is used for utility for network exploration and security auditing.

**h. Xplico**

Xplico is to fill in the data sent over the network from an application. Xplico can catch email using POP and SMTP protocols. Xplico can also capture all data sent using the HTTP protocol.

## IV. Implementation

The forensic goal is determined by the quality and quantity of information collected. Log files can be an important source of information for the forensic process. Log files contain information about various system resources, processes and user activity. Protocol analyzer, sniffer, SMTP, DHCP, FTP and WWW, router, firewall, and almost all system activity or a user can be collected in a log file. But if the system administrator can not be recorded, then the facts needed to connect actors with no incidents. Unfortunately, the clever attackers and criminals know this and its first objective is damage or alter log files to hide their activities.

The further need is the system clock. Recording a file associated with a time stamp and date stamp that allows the forensic analyst to determine the sequence of events. But if the system clock is not corrected / calibrated periodically can be turned off from anywhere from a few seconds up to several hours. It makes a problem because the correlation between log files from different computers that have different clock system would make it difficult if not impossible to correlate events. The simple solution to synchronize clocks across server and the system is running on a UNIX daemon like NTP daemon, which synchronizes system time and date on a regular basis with an atomic clock that is sponsored by the government.

### *A. Network Traffic Interpretation*

To be able to identify abnormal network traffic and suspicious, should be able to identify with both normal network traffic patterns. If the normal traffic pattern is not the indication is usually the source IP address looks unusual because it is a set of IP addresses reserve normally used in the network as a private address and never appeared on the internet. Also time-stamp too close together, and the source port and the serial number that rises uniformly is an indication that this is a package that is not normal. This package becomes SYNflood, a type of DoS (denial of service), an attack on these servers using port 139 (NetBIOS).

### *B. Time Lining*

Modified Access Creation time is a very useful tool to determine changes in the file, which can be used to create time lining of events.M-times information about when the file was last modified time, A-times contain information on the last access time, and C-times shows the last time the file status changed.

For example, where the access time and modification time and the time of conversion the same four minutes later show the change in ownership or permissions after the file is created. It also shows the file owner, size, licensing, the number of blocks used, the inode number and the number of links to the file.

## V. Conclusion

Network forensic is an important process to determine the crime. The digital evidence can be used for further investigation.Conclusions will be obtained when all the phases passed, regardless of the amount of evidence obtained or achieved the standard of truth. The materials here then that will be used as evidence for legal proceedings. Digital evidence tools have an important role in determining the error rate or gap errors that occur. Network forensics will examine more deeply the problems associated with network leakage, data theft, and network traffic. These phases are imperative because this is where the processes that have been done before rendering the truth and prove to the judge to disclose data and information events.

## References

[1]. B. Ruchandani, M. Kumar, A. Kumar, K. Kumari dan A. Sinha, “Experimentation In Network Forensics Analysis,” dalam Proceedings of the Term Paper Series under CDACCNIE, Bangalore, India, 2006.

[2]. A. Lubis dan A. P. U. Siahaan, “WLAN Penetration Examination of The University of Pembangunan Panca Budi,” International Journal of Engineering Trends and Technology, vol. 37, no. 3, pp. 165 - 168, 2016.

[3]. N. Meghanathan, S. R. Allam dan L. A. Moore, “Tools and Techniques for Network,” International Journal of Network Security & Its Applications, vol. 1, no. 1, pp. 14-25, 2009.

[4]. B.-H. Kang, “A Generic Framework for Network Forensics,” International Journal of Computer Applications, vol. 1, no. 11, pp. 1-6, 2010.

[5]. M. Cohen, “An Advanced Network Forensic Framework,” dalam The Digital Forensic Research Conference, USA, 2008.

[6]. M. T., B. B., B. T. M., R. Rajaram dan B. V. K., “Network Forensic Investigation of HTTPS Protocol,” International Journal of Modern Engineering Research, vol. 3, no. 5, pp. 3096-3106, 2013.

[7]. I. Riadi, J. E. Istiyanto, A. Ashari dan Subanar, “Log Analysis Techniques using Clustering in Network Forensics,” International Journal of Computer Science and Information Security, vol. 10, no. 7, 2012.