International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1): 74-81
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-001

# Forensics Analysis of Router On Computer Networks Using Live Forensics Method

Nita Hildayanti[1], Imam Riadi[2]
[1]*Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[2]*Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
*(nita1400018041@webmail.uad.ac.id, imam.riadi@is.uad.ac.id)*

**ABSTRACT**

One of hardware which is used for connecting two different networks is the Router. Router is a tool for sending data packets through a network or the internet in order to reach its object. In this research, an analysis of digital data collection was carried out and found the differences in the router data flow before and after the network is disconnected using Wireshark and Netcut. The research step starts from creating the scenarios that are often done on a daily basis where the user accesses the internet network from the router. At the results analysis, there are various types of data such as Internet Protocol who accesses, what is accessed, when user accesses, and where user accesses. Then find a comparison on the router data flow before and after the network is disconnected.

**Keyword** : *Live, Forensics, Router, Wireshark, Netcut*

## 1. INTRODUCTION

Digital forensics is a new science that develops continuously so it is necessary to deeply learn about this science. Digital forensics science changes because of the development of operating systems, smartphones and tablets. These big quantities and complex digital forensics steps require special capabilities and software to solve the problem that occurs. There are two general forensics digital analyzes, that are dead forensics and live forensics [1]. Dead forensics is a technique that requires data saved permanently in a hard disk general storage media device. Live forensics is an analysis technique which involves data that runs on a system or volatile data that is generally saved in the RAM or transit on the network [2] [3].

Network forensics is a branch of digital forensics related to monitoring and analyzing computer network traffic for gathering information, legal evidence or instructions detection. [4].

Live forensics can be done when the system is alive, because almost the entire system usage is saved in RAM, pagefile, hibernation files and crash dump files. An important purpose of analyzing data in RAM is to know the data location and the data contents. All datas on a computer must pass through RAM, whether it requires internet network, copy or move files, open files on the hard drive or delete them all recorded in RAM. The difference between RAM and Hard drive is, RAM records something that occurs at certain times and conditions while the hard drive only provides general data information. This is very important because there is only a large data and it never registers on a hard drive that is internet data [2] [5].

One of the most important devices on a network with a wide scope is a router. Routers can save the data traffic identity based on the tables which are available through the router. The transfer of information sources between networks on the router becomes the main concern to find the important data which is available in a connected network [6] [7].

The rapid progress of router technology proves that routers are the most needed device for companies, schools and universities, therefore each organization has important data that has been connected to the internet network, so crime may occur. For intruders, routers are very important to launch their actions so they can enter the main system or data center that they want to commit a crime. Full control of the router causes other networks connected to the router to be controlled. This is why many attackers will target the router and launch attacks against them. These attacks can focus on configuration errors, known vulnerabilities, or even weak passwords. Routers can be attacked by gaining access to the router and changing file configuration, launching attacks, flooding

bandwidth, or poisoning routing tables. If the router is successfully controlled, the configuration can be removed [6].

The use of routers to open free internet is starting to grow rapidly, there are free internet spots to encrypted hotspot or wifi logins everywhere. The presence of Netcut in the middle of the public makes the users of the wifi facility uneasy because all the bandwidth can be used by the perpetrator to do what they want to be able to cut the connection so that the perpetrator's computer is connected to the network, this action makes the facilities provided cannot be used by other users. Even with this software the perpetrator is able to turn off the router connection so the connection is off.

## 2. LITERATURE REVIEW

The research conducted by [8] this study examines e-mail security on proprietary systems, by comparing the e-mail security from gmail, ymail and outlook using Live Forensics method.

The research conducted by [6] this study analyzes DdoS attacks by utilizing an attack detection system using Intrusion Detection system (IDS) on routers to be able to find and collect digital evidence, using Intrusion Detection System (IDS) method.

The research conducted by [7] this study analyzes forensic by using logs for investigations and found evidence of an attack. The result of the study shows that by utilizing Basic Analysis and Security engine and Wireshark that are able to detect the attacks using rules in the snort which are the basis of attack evidence

The research conducted [9] this research finds a log of user activity, to be used as evidence in determining the best forensic method tools. Investigating volatile data on the systems running in RAM can find out logs of user activity. Data that can be used as evidence can be obtained from file system metadata, prefetch files, registry, web browser files and specific document files. The cases are scenarios with crimes that often appear and utilize freeware tools.

The research conducted by [10] this study implements live forensics techniques to investigate digital evidence of the activity of using Instant Messenger application, knowing the characteristics of digital evidence from the activities of using Instant Messenger application and making comparisons among Instant Messenger applications

The research conducted by [11] the aim of this study is to determine the network source attacks based on the log data, evidence, identification, analysis, and events reconstruction, computer networks security from attacks, based on the test results and analysis of computer network security system can be designed using computer network forensic evidence. And after creating a computer network security system, attackers will not be able to carry out attacks in the future using the same method.

## 3. THEORETICAL FRAMEWORK

### 3.1 Network Forensics

Network forensics is the activity of capturing, recording and analyzing events on the network to find security attack sources or others [12]. The forensics power allows analysis and retrievals the facts and events from the environment, because facts may be hidden. Unlike forensic in general, computer forensics is the activity of collecting and analyzing data from various computer resources. Logs that come from a computer (computer forensics) are antivirus logs, database logs or logs from applications used [13].

Network forensics is a part of digital forensics, which the evidence is captured from the network and interpreted based on the knowledge from network forensics. This research has some purpose that are to find out what data is obtained during the network is connected and then collect and analyze data from computer networks [11].

### 3.2 Live Forensics

Live forensics is an analytical technique which involves data running on a system or volatile data that is generally save in Random Access Memory (RAM) or transit on a network [8]. Live Forensics techniques require precision and accuracy, because the volitile data on RAM can be lost if the system is off, and there is a possibility of strucking down the important data in RAM by other applications [10].

Live forensics has similarities to the traditional forensics techniques in the methods used, that are identification, storage, analysis, and presentation, but live forensics is a response

from a lack of the traditional forensics techniques that cannot get information from the data and the information only exists when the system is running. For example memory activities, network processes, swap files, running system processes, and information from system files [14] [9].

The purpose of live forensics method is to deal with the incidents quickly, data integrity is more assured, encryption techniques are more likely to be opened and memory capacity is more lace when compared with the traditional forensics methods. Many tools can be used in live forensics for data analysis. Tools that are compared to the live forensics method are from memory usage capability, time, number of steps and the best accuracy in performing live forensics [15].

### 3.3 Forensics Stages

Generally, there are four stages which must be done in managing evidence for network forensics, that are collection, examination, analysis, and reporting.


Figure 1. Forensics Stages

In Figure 1, forensics stages can be explained that the network forensics stage method begins with a collection or called collecting data packets on the internet network. The next stage is examination. It is a process for checking the relevant data packets, then analysis stage is the stage to determine the complexity level of the data packet obtained, and the last stage is reporting. It is reporting and explaining what has been analyzed, then presented the data packets has been found and documented in detail.

### 3.4 *Router*

Router is a network device that is used to connect two different networks. A router is a tool for sending data packets over a network or the internet the internet in order to reach its object, the process is called routing.

Router will look for the best path to send a message based on the object address and origin address. Router knows the address of each computer in its local network, bridges and other routers [16].

### 3.5 *Netcut*

Netcut is a tool that is used for breaking the user's internet connection in a LAN/Hotspot area, to divert or disconnect the flow of data packets between users and the gateway [17].

### 3.6 *Wireshark*

Wireshark is commonly used in solving network troubleshooting to check network security, debug network protocol implementation in their software, debugging protocol package implementation, and protocol learning and also used for sniffers or sniffing privacy data on the network. Wireshark is like a media or tool that can be used by users for its use, whether for goodness or crime. This is because Wireshark can be used to search sensitive information that roams the network

Wireshark can analyze data packets in real time. It means that Wireshark application will oversee all data packets that come in and out through the interface that has been determined by the previous user and then display it.

If the computer is connected to a high-speed network and the computer is applying a network-based application, Wireshark application will display a lot of data packets and cause confusion because there are so many network data packets that occur. Wireshark application can filter certain types of protocols that you want to display [18].

## 4. METHODOLOGY AND EXPERIMENTAL SETUP

### 4.1 System Architecture

In the first scenario, forensic information is found on IP = 172.10.70.18, which is connected to the computer network, that are the IP who is accessing, what is accessed on, when user accesses, and where user accesses. Then analyze what happens to the router when the internet network is stable.

in the second scenario, the network is terminated using netcut at the IP = 172.10.70.18 then find the forensics data, that are the IP who is accessing, what is accessed, when user accesses, where user accesses and whether the information is still obtained after the network is

disconnected, then analyze what happens to the router when the internet network has disconnected.

### 4.2 Forensics Simulation on the Router

The simulation process of taking the forensics information on the router is by using three computers connected to the internet network which will be accessed. The simulation starts using one computer as a user, one computer as an attacker and one computer as an observer. The user's computer will access the internet, while the attacker will disconnect the internet network on the user's computer using Netcut, then the observer will observe the flow of internet network data when the user's computer is still connected to the internet network and when the user's computer has been disconnected to the internet network, observers also find out the forensics data obtained from the user's computer.

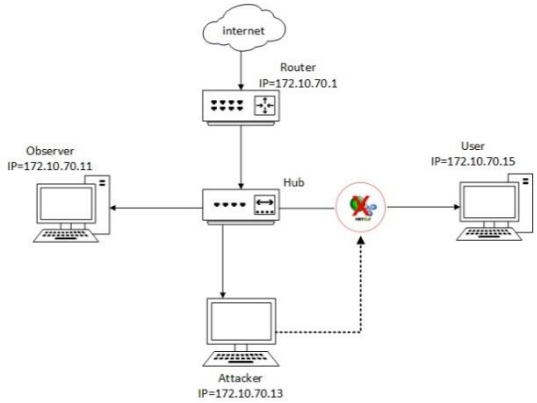


Figure 2. Experiment Scenario of Forensics Analysis

Figure 2 shows the experiment scenario of forensics analysis where the router with IP 172.10.70.1 sends data packets through the network or the internet to the HUB that will share to the observe computer IP 172.10.70.11, the user's computer IP 172.10.70.15, and the attacker computer IP 172.10.70.13. Attacker with IP 172.10.70.13 terminate the network using Netcut on the user's computer with IP = 172.10.70.15 so the user's computer will no longer to connect to the internet network, and the observer will observe the data flow process on the user's computer.

### 4.3 The Step of Research Process

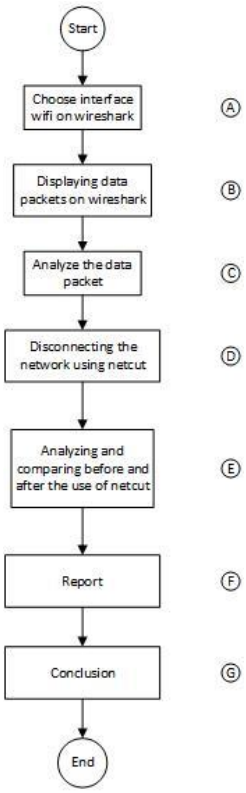


Figure 3. Collecting the Digital Data and the Comparison Between Before and After Using Netcut

Figure 3. shows the step of forensics analysis on the router that is getting data and comparing between before and after the computer network is disconnected using netcut software. This step of analysis consists of several processes, that are:

A. Opening an active wifi network toward Opening an active wifi network on Wireshark.
B. All network activities that are connected to the router will be recorded by Wireshark and will be displayed in packages.
C. Analyzing the packages displayed in Wireshark then find forensics information on network usage, that are the IP who is accessing, what is accessed, when he/she accesses, and where he/she accesses the internet network.
D. A computer internet network that has been determined to be analyzed will be disconnected using netcut software.

E. The next step is analyzing the computer network comparison before and after the network is disconnected using netcut software.
F. The report step is to report the results of the forensics analysis on the router, that is what is obtained from the analysis result and what is the result of the comparison of netcut usage on the computer network before and after the network is disconnected.
G. The conclusion step is what conclusions are expected from the results of the forensics analysis on the router.

### 4.4 Data Collection

The data collecting used in this research is recordings from Wireshark. The reconstruction process starts after the user accesses the computer network, then the user data will be displayed directly by Wireshark.

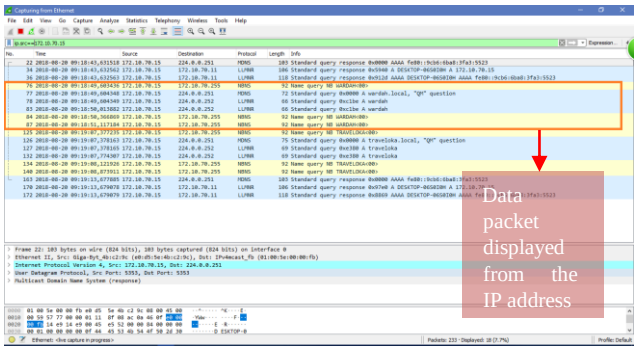


Figure 4. The Display of IP Packet = 172.10.70.15

In Figure 4, is known that the data packets in the red block are data packets from IP = 172.10.70.15, displayed that the internet user data with IP = 172.10.70.15 is accessing the internet on 20-08-2018, at 09:18:49, In the protocol, is displayed the NBNS protocol that is the Netbios protocol. It is used by applications on the Windows OS that are used in the TCP protocol to send the data completely until the data actually reaches to the receiver.

### 4.5 The Termination of Network to Computer

In Figure 5, it is known that the IP in the red block is the user's computer with IP = 172.10.70.15 which has been terminated at 9:19:36 on 20-08-2018 using netcut software.

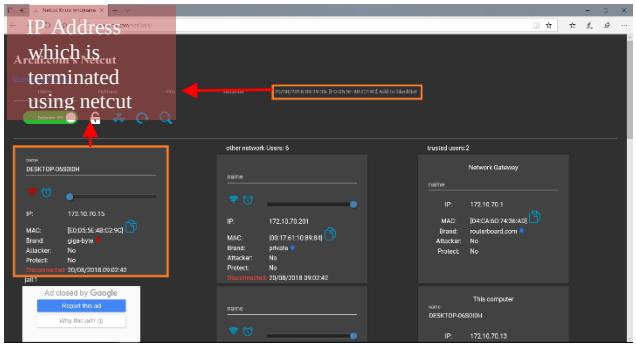


Figure 5. The Display When IP = 172.10.70.15 is Terminated Using Netcut

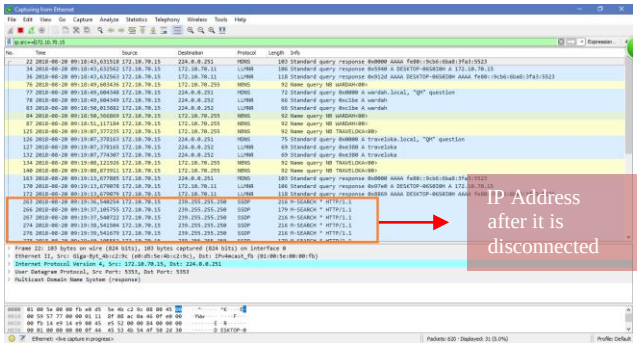


Figure 6. The Display of IP = 172.10.70.15 After the Internet Network is Disconnected Using Wireshark

In Figure 6, the data packets which is in the red block is the display of IP = 172.10.70.15, those data packets cannot display the data packets when the internet network at IP = 172.10.70.15 has been disconnected.

### 4.6 The Second Forensics Simulation On The Router

The simulation process of taking the forensics information on the router is by using three computers connected to the internet network which will be accessed. The simulation begins by using 1 computer as a user, 1 computer as an attacker and 1 computer as an observer, failed to get the forensics data after the internet network is terminated to the user's computer, so the second simulation is done which only uses two computers, one computer as a computer observers and attackers and one computer as a user. Computer users will access the internet, while computer observers and attackers will disconnect the internet network on the user's computer using Netcut and also

observe the process of data flow when it is still connected to the internet network and when the user's computer has been disconnected to the internet network, observers also find the forensics data obtained from User's computer using Wireshark.

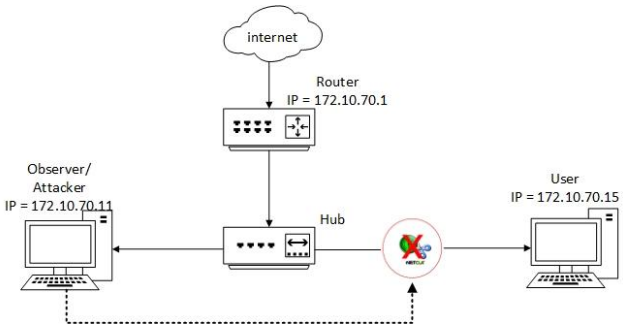


Figure 7. Experiment Scenario of Forensics Analysis

Figure 7 shows the experiment scenario of forensics analysis where the router with IP 172.10.70.1 sends data packets through the network or the internet to the HUB that will share to the observer/attacker computer IP 172.10.70.11 and the user's computer IP 172.10.70.15, then the computer with IP = 172.10.70.11 terminate the network using netcut on the user's computer with IP = 172.10.70.15 so the user's computer will no longer to connect to the internet network.

### 4.7 Data Collection

The data collecting used in this study is recordings from Wireshark. The reconstruction process starts after the user accesses the computer network, then the user data will be displayed directly by Wireshark.

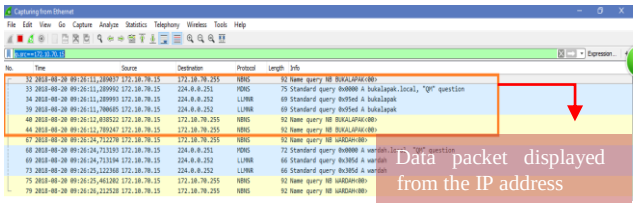


Figure 8. The Display of IP Packet = 172.10.70.15

In Figure 8, is known that the data packets in the red block are data packets from IP = 172.10.70.15, displayed that the internet user data with IP = 172.10.70.15 is accessing the internet on 20-08-2018, at 9:26:12, In the protocol, is displayed the NBNS protocol that is the Netbios protocol. It is used by applications on the Windows OS that are used in the TCP protocol to send the data completely until the data actually reaches to the receiver.

### 4.8 The Termination of Network to Computer

In Figure 9, is known that the IP in the red block is the user's computer with IP = 172.10.70.15 which has been terminated at 9:27:02 on 20-08-2018 using Netcut.

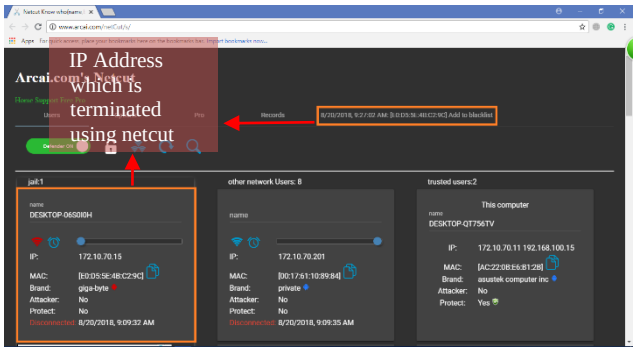


Figure 9. The Display when IP = 172.10.70.15 is Terminated Using Netcut

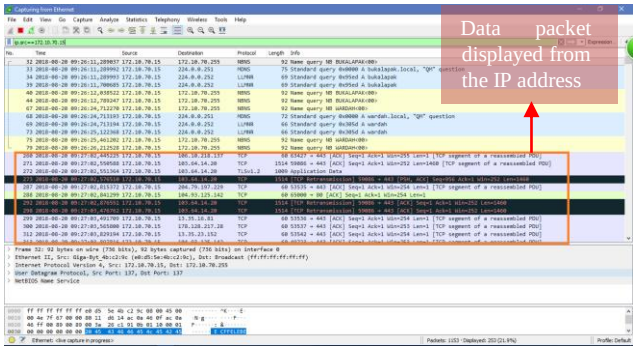


Figure 10. The Display of IP = 172.10.70.15 After the Internet Network is Disconnected Using Wireshark

In Figure 10, the data packet in the red block is displayed when IP = 172.10.70.15, on 20-08-2018, at 9:27:02, starts to be unstable, where the IP always asks a request to DNS then DNS cannot respond the request from the user IP so the next protocol that is displayed is the TCP protocol which means that the TCP protocol cannot send the data completely to the recipient so, TCP will always repeat because the data that will be sent to the recipient has an error.

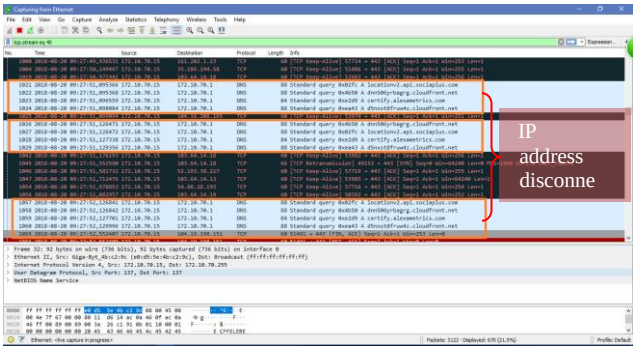


Figure 11. The Display of IP = 172.10.70.15 After the Internet Network is Off Using Wireshark

In Figure 11, the data packet in the red block is IP = 172.10.70.15 after the internet network is off, the IP always asks a DNS request, but DNS cannot respond so DNS will always repeat continuously.

### 4.9 Analysis and Comparison

In this step, present an analysis of the simulation results that have been done, the results of the analysis are in the form of any data obtained from the research results and what happens to the forensics router when the network is stable and when the network has disconnected, these are the following forensics data:

From the first simulation of forensic data that has been obtained, the internet user data with IP = 172.10.70.15 is accessing the internet on 20-08-2018, at 9:26:12, and the info displays the word "Bukalapak", in this simulation the use of the internet on the router is still running stable where requests from IP to DNS occur only one time to continue to the object domain, Then the TCP protocol will use the NBNS protocol to send the data completely until the data actually reaches to the receiver.

Next, in the second simulation where there has been a network termination using netcut software, on this network termination the forensics data that has been obtained is internet user data with IP = 172.10.70.15, on 20-08-2018, at 9:27:02, and the last object IP = 103.64.14.20, in this simulation the internet user on the router has lost an internet connection where the IP has asked a request for DNS and there is no response so the request occurs continuously from IP to DNS, Then TCP protocol will be displayed continuously because the data sent by TCP to the receiver has an error, so the data cannot reach to the receiver completely.

Then in the comparison step of the research results is comparing the first simulation before the internet connection is interrupted and the second simulation after the internet connection has been disconnected, the result of the simulation comparison is where the request from IP to DNS occurs only one time to continue to the object domain, this condition is different when the IP is done by terminating the network using netcut, then there will be a continuous request from IP to DNS.

## 5. RESULT ANALYSIS

### 5.1 User Acceptance Test (UAT)

User Acceptance Test (UAT) is a user testing process which is meant for producing documents that are used as an evidence of the analysis has been accepted by the user. The test is done using the simulation process of forensics data collecting analysis and what happens to forensics router when the network is stable and when the network has been disconnected using a video that has been documented during the research.

Some questions from testing User Acceptance Test are : the user knows the IP that accesses the network router, the user knows when the IP accesses the network router, the user knows what is accessed by another IP, the user knows what happened to the router when the network is disconnected and the user knows the difference before and after the network is disconnected.

From the results of the User Acceptance Test assessment, it can be conclude that: Analysis observers who have chosen Disagree are (0%), Analysis observers who have chosen Less Disagree are (9%), Analysis observers who have chosen Agree get (29%), Analysis observers who have chosen Strongly Agree get (12%).

## 6. CONCLUSION

Finding the data in the forensics router, helping in providing information about internet usage that is done by other users, so the use of the internet is not misused for bad purposes. Giving the information that occurs on the router data stream before and after the network is

disconnected then understanding the difference from both of them.

This research analyzes Netcut attacks by using Wireshark as an attack detector. In the previous research, the attacks used DdoS and Intrusion Detection System (IDS) as an attack detector. So, this research provides information that occurs on the router data flow when it is connected to the internet network and after being disconnected from using Netcut then knowing the difference when the data flow Router is connected to the internet and when the data flow Router is disconnected using Netcut.

The result of the simulation comparison is where the request from IP to DNS occurs only one time to continue to the object domain, this condition is different when the IP is done by terminating the network using netcut, then there will be a continuous request from IP to DNS.

## REFERENCES

[1] M. Kolhe and P. Ahirao, "Live Vs Dead Computer Forensic Image Acquisition," *Int. J. Comput. Sci. Inf. Technol.*, vol. 8, no. 3, pp. 455–457, 2017.

[2] M. Nur Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," *JISKa*, vol. 1, no. 3, pp. 108–114, 2017.

[3] S. A. Mandowen, "Analisis forensik komputer pada lalu lintas jaringan 1," *J. Sains*, vol. 16, no. 1, pp. 14–20, 2016.

[4] F. Budiharjo, Suyatno; Riyadi, "Forensik Jaringan Pada Lalu Lintas Data Dalam Jaringan Honeynet di Indonesia Security Incident Respone Team On Internet Inflastructure/Coordination Center," vol. 13, no. 2, pp. 125–136, 2014.

[5] Soni, Y. Prayudi, and B. Sugiantoro, "Teknik Akuisisi Virtualisasi Server Menggunakan Metode Live Forensic," *Teknomatika*, vol. 9, no. 2, 2017.

[6] F. Ridho, A. Yudhana, and I. Riadi, "Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time," vol. 2, no. 1, pp. 111–116, 2016.

[7] F. Ridho, A. Yudhana, and I. Riadi, "Implementasi Log Dalam Forensik Router Terhadap Serangan Distributed Denial of Service ( DDoS )," vol. VI, no. 2, pp. 15–21, 2017.

[8] M. N. Faiz, R. Umar, A. Yudhana, and U. A. Dahlan, "Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary," *J. Ilm. Ilk.*, vol. 8, no. 3, pp. 242–247, 2016.

[9] R. Umar, A. Yudhana, and M. N. Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," *Pros. Konf. Nas. Ke- 4 Asos. Progr. Pascasarj. Perguru. Tinggi Muhammadiyah*, no. April, pp. 207–211, 2016.

[10] T. D. Larasati and B. C. Hidayanto, "Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10," *Sesindo*, vol. 6, no. November, pp. 456–256, 2017.

[11] S. Fadlil, Abdul; Riadi, Imam; Aji, "Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan," *J. Ilmu Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, pp. 12–19, 2017.

[12] J. Fahana, R. Umar, and F. Ridho, "Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan," *Query J. Inf. Syst.*, vol. 1, no. 2, pp. 6–14, 2017.

[13] E. K. Dewi, "Analisis Log Snort Menggunakan Network Forensic," *JIPI (Jurnal Ilm. Penelit. dan …*, vol. 02, pp. 72–79, 2017.

[14] M. S. Ahmad, I. Riadi, and Y. Prayudi, "Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Serangan Man in the Middle Attack Berbasis Evil Twin," *Ilk. J. Ilm.*, vol. 9, no. April, pp. 1–8, 2017.

[15] D. S. Yudhistira, "Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop," 2018.

[16] N. Feby Puspitasari, "Implementasi Mikrotik Sebagai Solusi Router Murah Dan Mudah," *Semin. Nas. Teknol. (SNT 2007)*, vol. 2007, no. November, pp. D1–D14, 2007.

[17] M. Akbar, "Perancangan Software Ids Snort Untuk Pendeteksian Serangan Interruption ( Netcut ) Pada Jaringan Wireless," *Instek*, Vol. 3, No. 1, 2018.

[18] T. M. Diansyah, J. T. Informatika, S. Tinggi, and T. Harapan, "Analisa pencegahan aktivitas ilegal didalam jaringan menggunakan wireshark," *Anal. Pencegah. Akt. Ilegal Di Dalam Jar. Menggunakan wireshark*, vol. IV, no. 2, pp. 20–23, 2015.