Live Forensics on RouterOS using API Services to Investigate Network Attacks

By Imam Riadi

WORD COUNT	3754	TIME SUBMITTED	18-JUL-2017 03:55PM
		PAPER ID	30577414

Live Forensics on RouterOS using API Services to Investigate Network Attacks

Muhammad Itqan Mazdadi
Department of Informatics Engineering
Islamic University of Indonesia
Yogyakarta, Indonesia
itqanmazdadi@gmail.com

Imam Riadi
Department of Information System
Ahmad Dahlan University
Yogyakarta, Indonesia
imamriadi@is.uad.ac.id

Ahmad Luthfi
Department of Informatics Engineering
Islamic University of Indonesia
Yogyakarta, Indonesia
ahmad.luthfi@uii.ac.id

***Abstract*— Network Forensics are complicated and worth studying. One of the interesting parts of the network is a router that manages all connection for all logical network activity. On network forensics, we need traffic log to analyze the activity of any computer connected to the network in purpose to know what hackers do. In another hand, not all information can get from traffic log if the network didn't save the network sniffing. Thus this case need find other resources like router information. To access information on the router like RouterOS on Mikrotik devices, can maintain some data using API to remote access the router remotely. The purpose of this paper is to explore how to do a forensics of RouterOS based Mikrotik devices and developing a remote application to extract router data using API services. As a result, acquisition process could obtain some valuable data from the router as digital evidence to explore information of network's attacks activity.**

Keywords- Network; Router; Live Forensics; API; Logs

I. Introduction

Network forensics is part of the digital forensics that focuses on monitoring and analysis of data traffic on the network. The type of data being handled is dynamic data network forensics. It is different to that of digital forensics, data which are static[1][2]. With the increasing presence of digital devices, information storage, and network traffic, forensics Cyber face of the growing number of cases that have complex growth.

Digital evidence is always taken from the network traffic logs derived from sniffing or monitoring activity to be analyzed[2][3]. In addition to the actual network traffic logs of the router device, we can also get some valuable information to a network. Information may be found on the router is admin logging activity, a list of client IP address, mac address, network configuration, firewall configuration, etc.

API (Application Programming Interface) is a set, functions, and protocols that can be used by programmers when building software for a particular operating system. API allows programmers to use standard functions to interact with other operating systems. API is one method of doing abstraction, usually (but not always) between the low-level software and high-level. RouterOS Mikrotik API began in introduced and used since version 3.0 [4][5].

Under the background of the domains that have been presented, this study is to gather information and conduct an analysis of digital evidence contained in the RouterOS by using the API (Application Programming Interface) as a tool to help maintain information on the activity of network forensics.

II. Related Works

Several previous studies have been done on digital forensics. Research about Logs management system has been developing for several years like kiwi syslog, bnare backlog, spectorosoft server manager, manage engine, and splunk log management[6]. The management log system helps forensics investigators to analyze and determine an approach to detect network attacks[7]. The most useful research on network forensics is the development of method ontology for intelligent network forensics analysis[8].

Some research about router forensics has done on several router devices like Cisco, TP-Link, Ubiquity etc. Most of the study of router forensics is included DHCP handling in determining IP address of computer client that extracted on device memory[9]. Not only on physical devices, but some virtual model of the router also given some information for digital forensics[10].

Acquisition of data from the Household and Small Business Wireless Router also provides an overview of how the retrieval of data from the router. In addition they also mapped the correlations NAT TCP flow on private wireless networks between TCP flow to the internet. As well as the mechanism of relationship logging IP and TCP port[11].

III. Basic Theory

A. Network Forensics

Network forensics is a forensic field that focuses on the area of network and associated devices. Network forensics is an attempt to find the attacker information to look for potential evidence after an attack or incident. There is a variety kind of attacks include probing, DoS, user to root (U2R) and remote to local. Network forensics is the process of capturing, annotating and analyzing network activity in order to find digital evidence of an attack or crime committed using a computer network.

Digital evidence from the network can be identified from the recognized attack patterns and deviations from normal behavior. Network forensics has a variety of activities and techniques of analysis, such as analysis of existing processes in the IDS , the analysis of network traffic and the analysis of network device itself, all considered the part of a network forensics[2].

B. *Live Forensics Method*

Live forensic is a method of forensics used when the system is in running state. This is because the data that will be withdrawn likely lost when the system is turned off. The implementation of live forensic usually used in the case of volatile memory. Volatile data is the data that usually stored in temporary media like RAM, where is very easily to lost. The volatile data acquisition process should be implemented as soon as possible after the incident. The live forensic method is required in a case of acquisition of log server and computer RAM.

One of the problems that happen to live forensic is the modification of data or contamination data, it because the acquisition process is done on the system itself. In the case of taking the Log on the server, the servers also keep records on the log of acquisitions activity. Even so, the forensic examiners must be competent and understand implications of their actions [12].

C. *Mikrotik RouterOS*

Mikrotik is a Linux-based operating systems on a computer that functioned as a router[12]. It designed to manage the network in small-scale networks like home and large-scale network like an office. Mikrotik began to be established in 1995 that was originally intended for the company's Internet service (Internet Service Provider, ISP). Currently, MikroTik provides services to many wireless ISPs for Internet access services in many countries around the world and also very popular in Indonesia[13].

Mikrotik on standards-based hardware Personal Computer (PC) known for their stability, quality control and flexibility for different types of data packets and handling of these processes (routing). Mikrotik created as a router-based computer much benefit for an ISP that wants to run multiple applications ranging from the lightest to advance. In addition to routing, Mikrotik can be used as a management access capacity, bandwidth control, firewall, hotspot system, Virtual Private Network server and much more[13].

D. *API (Application Programming Interface)*

API (Application Programming Interface) is a set of commands, functions, and protocols that can be used by programmers when building software for a particular operating system. API allows programmers to use standard functions to interact with other operating systems[4][10][14]. The concept of API model shown in figure 1:

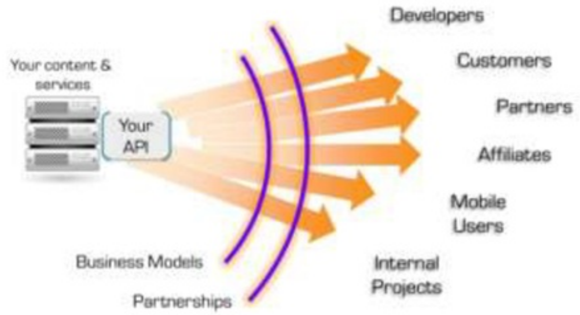


Figure 1. Use of API

One of the benefits of the API is to provide convenience to developers to create applications that can communicate to the device through a wide variety of programming languages. RouterOS has provided an API Services that can be used to communicate custom software to the router devices. The developers can create their own applications to suit their needs. The API services on RouterOS can be applied to the programming language like Java, PHP, pearl, C ++, etc[4][5].

IV. System Requrement

To support the experiment on this research, the hardware and software that necessary used is listed below:

- Mikrotik RB750 with RouterOS version 6
- Access Point TP-Link MR3020
- ADSL Modem as Source Internet
- Laptops, PC, and Smartphone as client on the network
- Java SDK
- Netbeans for software development

The Network topology implemented on this research illustrated by figure 2:

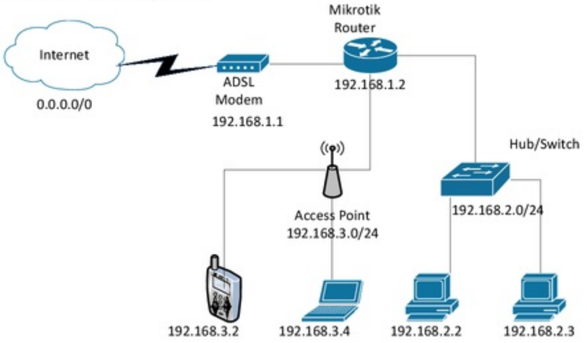


Figure 2. Network Topology

This topology applies router Mikrotik RB750 to distribute internet access from ADSL Modem to client trough Switch/Hub and Access Point. Switch/Hub is a bridge for connecting PC to the router using wired LAN Port. Access Point is used to connecting Laptops and Smartphone using wireless connectivity.

V. ACQUISITION TOOL DEVELOPMENT

Refers to the analysis of digital evidence on the common router from related research, we determine what information need to be extracted from RouterOS. The information that should be capable of being extracted is Log activity, ARP, IP Address, DHCP Leases, RouterBoard Info, and DNS Cache.

On RouterOS version 6, the API service is automatically active as the default configuration. The API allow the software that we develop to maintain data from the router using communication protocol on port 8763[4]. Workflow of developed application show by figure 3:

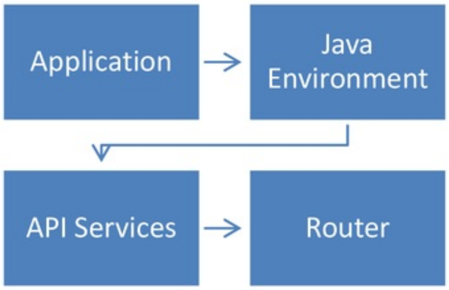
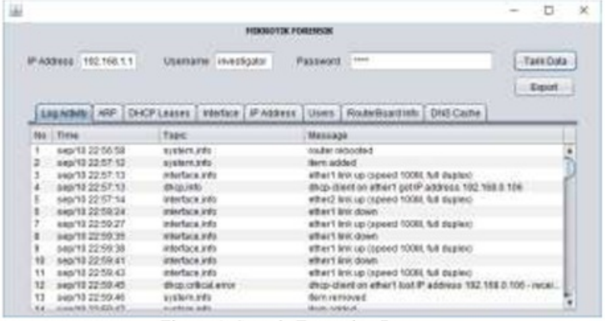


Figure 3 Process Workflow

The software is built with one simple form as the main menu. To perform data extraction, the investigator needs to input IP Address of Router, Username, and Password. After that, the tables on the form will show the extraction data. The data is categorized by tabulation bar for each field. Sample result of data acquisition shown in Figure 4:



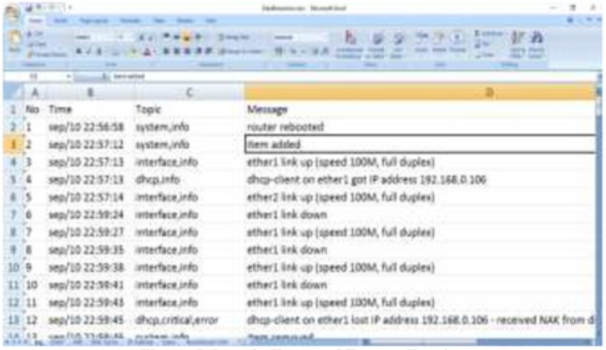
IP Address 192.168.1.1 Username investigator Password ****

No	Time	Topic	Message
1	sep/10 22:56:58	system,info	router rebooted
2	sep/10 22:57:12	system,info	item added
3	sep/10 22:57:13	interface,info	ether1 link up (speed 100M, full duplex)
4	sep/10 22:57:13	dhcp,info	dhcp-client on ether1 got IP address 192.168.0.106
5	sep/10 22:57:14	interface,info	ether2 link up (speed 100M, full duplex)
6	sep/10 22:59:24	interface,info	ether1 link down
7	sep/10 22:59:27	interface,info	ether1 link up (speed 100M, full duplex)
8	sep/10 22:59:35	interface,info	ether1 link down
9	sep/10 22:59:38	interface,info	ether1 link up (speed 100M, full duplex)
10	sep/10 22:59:41	interface,info	ether1 link down
11	sep/10 22:59:43	interface,info	ether1 link up (speed 100M, full duplex)
12	sep/10 22:59:45	dhcp,critical,error	dhcp-client on ether1 lost IP address 192.168.0.106 - recei...
13	sep/10 22:59:46	system,info	item removed

Figure 4. Sample Extraction Process

The extracted data show separately by tab based on the information categories. The categories tab is Log Activity, IP address List , ARP, DHCP Leases, RouterBoard Info, Users, and DNS Cache.

For the purposes of analysis, export feature is added to allow extracted data export as .xlsx spreadsheet file. This xlsx file can be used as digital evidence for analysis. The sample of exported .xlsx file shown in figure 5.



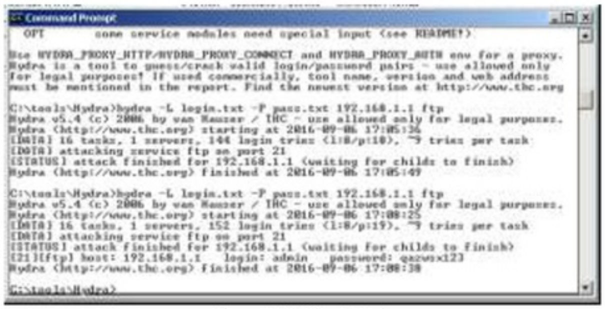
No	Time	Topic	Message
1	sep/10 22:56:58	system,info	router rebooted
2	sep/10 22:57:12	system,info	item added
3	sep/10 22:57:13	interface,info	ether1 link up (speed 100M, full duplex)
4	sep/10 22:57:13	dhcp,info	dhcp-client on ether1 got IP address 192.168.0.106
5	sep/10 22:57:14	interface,info	ether2 link up (speed 100M, full duplex)
6	sep/10 22:59:24	interface,info	ether1 link down
7	sep/10 22:59:27	interface,info	ether1 link up (speed 100M, full duplex)
8	sep/10 22:59:35	interface,info	ether1 link down
9	sep/10 22:59:38	interface,info	ether1 link up (speed 100M, full duplex)
10	sep/10 22:59:41	interface,info	ether1 link down
11	sep/10 22:59:43	interface,info	ether1 link up (speed 100M, full duplex)
12	sep/10 22:59:45	dhcp,critical,error	dhcp-client on ether1 lost IP address 192.168.0.106 - received NAK from d

Figure 5 Sample Exported Data to Excel

VI. TEST AND RESULT

A. Attack Simulation Test

On simulation stage, we perform an attack on the router using hydra tool. The purpose of this attack is to leave some footprint on the router of some attack activity. Hydra is a tool to maintain attack via network services like FTP Service. Using "dictionary attack" method, hydra obtains login based on dictionary of username and password. Hydra will do several login requests until the login is success gained or fail if no one username and password is match with dictionary list. Hydra is used by CLI (Command line interface) as shown in figure 6:



```
  OPT       some service modules need special input (see README!)

Use HYDRA_PROXY_HTTP/HYDRA_PROXY_CONNECT and HYDRA_PROXY_AUTH env for a proxy.
Hydra is a tool to guess/crack valid login/password pairs - use allowed only
for legal purposes! If used commercially, tool name, version and web address
must be mentioned in the report. Find the newest version at http://www.thc.org

C:\tools\Hydra>hydra -L login.txt -P pass.txt 192.168.1.1 ftp
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2016-09-06 17:05:36
[DATA] 16 tasks, 1 servers, 144 login tries (l:8/p:18), ~9 tries per task
[DATA] attacking service ftp on port 21
[STATUS] attack finished for 192.168.1.1 (waiting for childs to finish)
Hydra (http://www.thc.org) finished at 2016-09-06 17:05:49

C:\tools\Hydra>hydra -L login.txt -P pass.txt 192.168.1.1 ftp
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2016-09-06 17:08:25
[DATA] 16 tasks, 1 servers, 152 login tries (l:8/p:19), ~9 tries per task
[DATA] attacking service ftp on port 21
[STATUS] attack finished for 192.168.1.1 (waiting for childs to finish)
[21][ftp] host: 192.168.1.1   login: admin   password: qazwsx123
Hydra (http://www.thc.org) finished at 2016-09-06 17:08:38

C:\tools\Hydra>
```

Figure 6. Hydra Attack

In this case, it attacks router on address 192.168.1.1 via FTP services. The result is found that username is "admin" and password is "qazwsx123".

B. Acquisition & Analysis

The challenge of router forensic is about volatile data stored on the memory that will destroy after a reboot or the router shut down. This condition is the reason why the method of live forensics should be implemented in this process. The acquisition should be performing as soon as possible after the incident[15]. The acquisition is initiated on a computer that connected to the network as a client.

Using the application that been developed to extract the data from the router. The sample result of acquisition shown in table 1:

TABLE 1. SAMPLE DATA OF LOG ACTIVITY

Time	Topic	Message
16:07:31	system,error,critical	login failure for user pengelola from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user pengelola from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user pengelola from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user sa from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user sa from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user root from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user sa from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user root from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user administrator from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user administrator from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user root from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user administrator from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user administrator from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user pengelola from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user sa from 192.168.1.246 via ftp
16:07:31	system,error,critical	login failure for user root from 192.168.1.246 via ftp
16:07:32	system,error,critical	login failure for user power from 192.168.1.246 via ftp
16:07:32	system,error,critical	login failure for user power from 192.168.1.246 via ftp
16:07:32	system,error,critical	login failure for user power from 192.168.1.246 via ftp
16:07:32	system,error,critical	login failure for user kasir from 192.168.1.246 via ftp
16:07:32	system,error,critical	login failure for user power from 192.168.1.246 via ftp
16:07:33	system,error,critical	login failure for user admin from 192.168.1.246 via ftp
16:07:34	system,info, account	user admin logged out from 192.168.1.246 via ftp
16:08:46	system,info, account	user admin logged in from 192.168.1.246 via telnet
16:11:26	system,info	user jebol added by admin
16:12:51	system,info	simple queue changed by admin
16:13:29	system,info, account	user investigator logged in from 192.168.1.243 via api

The analysis process should be able to link information from different variable includes the completion of information against other information to explain an event or attacks activity. Stages of analysis data field shown in figure 7:

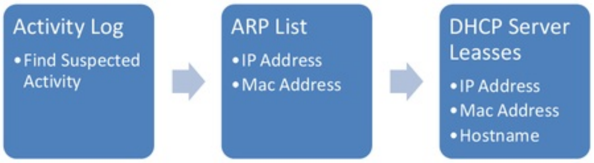

Activity Log
• Find Suspected Activity
ARP List
• IP Address
• Mac Address
DHCP Server Leasses
• IP Address
• Mac Address
• Hostname

Figure 7. Data Stages Analysis

Observation data starts with observing Log Activity on Table 1 that show the IP Address 192.168.1.246 has 38 failed login requests from time 16:07:30 until 16:07:32. This action is impossible as human behavior that can make 38 requests in 2 seconds. That makes 192.168.1.246 as suspected address. In 16:08:46 found that 192.168.1.246 is successfully logged in via telnet which means it gained full access to the router. The action is followed by an activity to add a new user to the router with name "jebol" at time 16:11:26.

For validation of attack activity, we collect the network log from the network sniffing. The sniffing process is recording the activity of traffic on the network. With tool named Wireshack, observe a .pcap file to explore FTP Services Communication activity as shown in figure 8. As expected, same FTP activity obtained from address 192.168.1.246 is found.

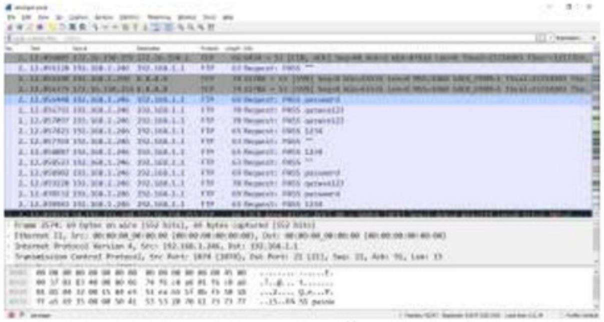


Figure 8. Observation Network Traffic Log with Wireshack

The search continued in subsequent data by looking the ARP list. ARP list shows information about IP address that is owned by a Mac Address on the network. Observation on the table 2 found that Mac Address of 192.168.1.246 is 00:0C:29:48:0B:0A.

TABLE 2. ARP LIST

IP Address	Mac Address	Interface
192.168.1.243	00:26:6C:98:CE:C3	ether2
172.16.150.1	00:1E:67:CF:1A:B1	ether1
192.168.1.242	CC:07:AB:8F:06:9D	ether2
192.168.1.254	14:F6:5A:67:CF:59	ether2
192.168.1.246	00:0C:29:48:0B:0A	ether2
192.168.1.251	74:2F:68:9D:26:35	ether2
192.168.1.249	00:21:5D:4C:D7:D0	ether2
192.168.1.250	60:D9:A0:64:36:2C	ether2

Note : The highlighted data colored by red.

In addition, to knowing the hostname of attacker computer and validate the address, DHCP Leases field needs to observe. The data of DHCP Leases shows at table 3:

TABLE 3. DHCP LEASES

IP Address	Mac Address	Host Name
192.168.1.245	58:A2:B5:82:5D:08	android-d803df206d5dfd68
192.168.1.244	54:27:1E:B8:98:EF	Falcon-00
192.168.1.241	74:29:AF:EB:17:CF	POLICE
192.168.1.242	CC:07:AB:8F:06:9D	android-ab0a5c691d5a4e06
192.168.1.246	00:0C:29:48:0B:0A	HACKER
192.168.1.248	74:E5:43:6E:4B:6D	Billy-PC
192.168.1.249	00:21:5D:4C:D7:D0	Puniyas
192.168.1.243	00:26:6C:98:CE:C3	mazda

Note : The highlighted data colored by red.

As the result of analysis, it reports that the attack is coming from PC with Name "HACKER". It has Mac address 00:0C:29:48:0B:0A with IP Address 192.168.1.246.

C. Reboot Test

In order to understand the characteristics of digital evidence on RouterOS, we perform reboot on router to test what kind information is still exist or lost. After the router is rebooted, we compare the information of *Activity Log, ARP, DHCP Leases, Interface, IP Address, Users, Routerbard Info, DNS Cache* before and after the reboot. As the result we found some information still exists but most of it is lost as explain at table 4.

TABLE 4 CHARACTERISTIC OF DIGITAL EVIDENCE ON ROUTEROS

No	Information Field	Behavior after reboot
1	*Activity Log*	Lost / volatile
2	*ARP*	Lost / volatile
3	*DHCP Leases*	Lost / volatile
4	*Interface*	Exist / Non-volatile
5	*IP Address*	Exist / Non-volatile
6	*Users*	Exist / Non-volatile
7	*Routerboard Info*	Exist / Non-volatile
8	*DNS Cache*	Lost / volatile

VII. CONCLUSIONS

Forensic against Router OS-based router devices can be done with methods of live forensics through the media API. Extraction of Router's data with API gives us access to information on a wide variety of activities that are on the network.

The developed application is success gained 9(nine) field of data from the router, which are Log Activity, IP address List, ARP, DHCP Leases, RouterBoard Info, Users, and DNS Cache. All of the data fields is used for observing network attack based on the scenario, but DNS Cache field role has no correlation with FTP Services Attack case scenario. Analysis of the connected links between any variable field on acquisition data can help digital forensic investigators to determine an activity and source of Attacks from Networks.

In order to avoid lost of information, the acquisition process of forensics should be perform as soon as possible before the Router turned off or rebooted.

VIII. FUTURE WORKS

The future works of the research is necessary to extend the knowledge of the current research. This paper is only maintaining information from internal network attack. For the future works, the exploration of forensics method to investigate attacks from different scheme of topology is necessary to obtain information of attack from external network or from the internet source.

REFERENCES

[1] A. Iswardani and I. Riadi, "Denial Of Service Log Analysis Using Density K-Mans Method," vol. 83, no. 2, pp. 299–302, 2016.

[2] I. R. Jazi, Eko Istiyanto, A. Ashari, and Subanar, "Internet Forensics Framework Based-on Clustering," *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 12, pp. 115–123, 2013.

[3] I. Riadi, J. Istiyanto, and a Ashari, "Log Analysis Techniques using Clustering in Network Forensics," *Int. J. Comput. Sci.*, vol. 10, no. 7, 2014.

[4] G. Stoitsov and V. Rangelov, "One implementation of API interface for RouterOS," vol. 3, no. 2, 2014.

[5] C. O'Halloran and D. Chambers, "Dynamic adaptation of OSPF interface metrics based on network load," *2015 26th Irish Signals Syst. Conf. ISSC 2015*, no. 89, 2015.

[6] A. Aeri and S. Tukadiya, "A comparative study of network based system log management tools," *2015 Int. Conf. Comput. Commun. Informatics*, pp. 1–6, 2015.

[7] K. Nguyen, D. Tran, W. Ma, and D. Sharma, "An approach to detect network attacks applied for network forensics," *2014 11th Int. Conf. Fuzzy Syst. Knowl. Discov. FSKD 2014*, pp. 655–660, 2014.

[8] S. Saad and I. Traore, "Method ontology for intelligent network forensics analysis," *PST 2010 2010 8th Int. Conf. Privacy, Secur. Trust*, pp. 7–14, 2010.

[9] T. Fiebig, "Forensic DHCP Information Extraction from Home Routers," 2013.

[10] X. Gao, X. Zhang, Z. Lu, and S. Ma, "A general model for the virtual router," *2013 15th IEEE Int. Conf. Commun. Technol.*, pp. 334–339, 2013.

[11] Z. Liu, Y. Chen, W. Yu, and X. Fu, "Generic network forensic data acquisition from household and small business wireless routers," *2010 IEEE Int. Symp. "A World Wireless, Mob. Multimed. Networks", WoWMoM 2010 - Digit. Proc.*, 2010.

[12] A. M. Saliu, "Internet Authentication and Billing (Hotspot) System Using MikroTik Router Operating System," *Int. J. Wirel. Commun. Mob. Comput.*, vol. 1, no. 1, p. 51, 2013.

[13] I. Riadi, "Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik Pendahuluan Landasan Teori," *JUSI, Univ. Ahmad Dahlan Yogyakarta*, vol. 1, no. 1, pp. 71–80, 2011.

[14] K. Liu and K. Xu, "Open service-aware mobile network API for 3rd party control of network QoS," *Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012*, vol. 1, pp. 172–175, 2012.

[15] B. T. Femalld and C. Lahaie, "Live System Forensics Patrick Leahy Center for Digital Investigation Champlain College."

Live Forensics on RouterOS using API Services to Investigate Network Attacks

ORIGINALITY REPORT

2%

SIMILARITY INDEX

PRIMARY SOURCES

1	www.pa-manna.go.id Internet	37 words — 1%
2	www.resolvedigital.co.nz Internet	24 words — 1%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		