ILKOM Jurnal Ilmiah Vol. 13, No. 2, August 2021, pp. 163-167
Accredited 2nd by RISTEKBRIN No. 200/M/KPT/2020; E-ISSN 2548-7779 | P-ISSN 2087-1716

Header investigation for spam email forensics using framework of national institute of standards and technology

Imam Riadi [a, 1, *]; Rusydi Umar [a, 2]; Mustafa [a, 3]
[a] *Universitas Ahmad Dahlan, Jl. Kapas No.9, Semaki, Kec. Umbulharjo, Kota Yogyakarta, Daerah Istimewa Yogyakarta 55166*
[1] *imam.riadi@is.uad.ac.id;* [2] *rusydi.umar@mti.uad.ac.id;* [3] *mustafa.ramliannor@gmail.com*
** Corresponding author*

Article history: Received April 29, 2021; Revised July 05, 2021; Accepted July 23, 2021; Available online August 07, 2021

Abstract

Today's technology makes communication very easy and can be used anywhere, even a distance of hundreds to thousands of kilometres is not a barrier in communicating. One of the tools or media that is widely used is via email. However, there are many disadvantages that may be obtained from the email, one of which is spamming or mail. The purpose of this research is to know the stages of spamming email analysis through header analysis. The method used in this study is the National Institute of Standards and Technology (NIST) and this method uses 4 stages, namely collection, examination, analysis, and reporting. The results of this study are expected to be able to find out the spam sender's email address, the spam email sender's IP address, and other information needed.

Keywords: Digital Forensics; Forensic e-mail; Forensic Tools; NIST

Introduction

Nowadays internet services make it easy for humans to do all their activities anywhere and anytime. This convenience is fortified by the reach of the internet that goes beyond various boundaries that makes the growth of the internet very fast every day [1]. One of the internet services that is widely used and very popular is e-mail which is used in an organizational, corporate or individual environment [2]. With technological developments, e-mail is not only able to send text files, but can also send several files such as audio, video, photo, and other extension files [3]. There are threats that follow by utilizing these features as a medium of crime in the cyber world, because email is the easiest tool to become a medium for sending spam (phishing, scam, malware, computer viruses and mail worms) and malicious programs that are camouflaged and attached to attachments. One of the crimes found involving email was email spamming and email spoofing [4]. Spamming is the sending of unwanted news or advertisements or what is called bulk mail or junk email [5]. While email spoofing is an email that is intentionally faked so that it seems as if it was sent from a legitimate email [6].

With so many crimes happening today, more and more technologies are being developed to check and protect e-mails, including spam e-mail detection [7]. One way to develop this technology is to conduct internet forensic investigations [8]. The results of testing and analysis on the system are designed for useful forensic evidence [9]. In general, there are two types of internet forensic investigations, namely dead forensics and live forensics [10]. Dead forensics is a technique that requires data to be stored permanently in a storage media device, generally a hard disk. Live forensics is an analytical technique that involves running data which is generally stored in Random Access Memory (RAM) or in transit on a network [11]. An important part in digital forensics is the authenticity of digital evidence [12]. Conducting an investigation through the stages of a digital forensics digital examination procedure approach is the correct way to obtain the evidence [13].

The National Institute of Standards and Technology (NIST) is a method used to perform forensic analysis. This method has been widely used as a reference for forensic analysis research. For example, in android-based analysis, Wijaya (2017) used the NIST method to analyze the telegram application on smartphones [14]. Also, Anshori (2018) analyzed the digital evidence for Facebook Messenger which also used the NIST method [15].

This research can later become new knowledge about how forensic investigations deal with crimes in the cyber world, especially in the case of e-mail spam. As in the real world, crimes in the cyber world also require a forensic process, which combines elements of law and computer science. This research can be a first step to solving a complex crime case and can help with previous research. E-mail header investigation is an important aspect of

http://dx.doi.org/10.33096/ilkom.v13i2.849.163-167

investigation because e-mail metadata and other information are contained in e-mail headers. Analysis of e-mail headers can reveal the source, destination, e-mail client, sender IP, identification of fake or authentic e-mails, and more. In practice, e-mails have been repeatedly adopted as evidence by legal departments. With the continuous advancement of national legal processes and the continuous improvement of electronic evidence laws, e-mail forensics is indispensable in the detection of computer crime cases.

Method

The analysis process of this research uses the National Institute of Standards and Technology (NIST) method. This method refers to the basic stages in a forensic analysis, namely collection, examination, analysis, and reporting [16] which is shown in **Figure 1**.

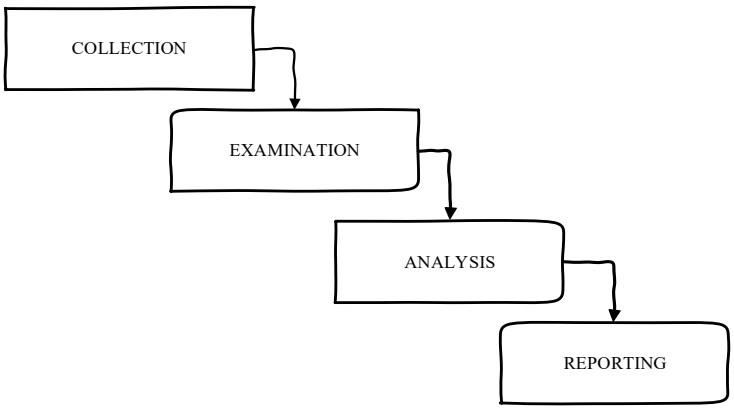

Figure 1. Stages in the method National Institute of Standards and Technology (NIST)

A. Collection

Collection was the stage of conducting the forensic process to identify sources that are considered potential to be used as evidence, and the steps needed in data collection.

B. Examination

Examination was the stage of processing the data collected forensically, either automatically or manually.

C. Analysis

Analysis was the stage of analyzing the results of the examination using technically and legally justified methods to obtain useful information and answer questions that encourage collection and examination.

D. Reporting

The reporting stage was reporting the results of the analysis which includes a description of the actions taken.

Results and Discussion

The results of this study were earned through evidences on spam emails by opening the header in the email.

A. Collection

This stage was the stage for identifying the header section for digital evidence and conducting data sources. The first step in the forensic process was to identify sources that were considered potential to be used as evidence. Further, we described the steps required in data collection.

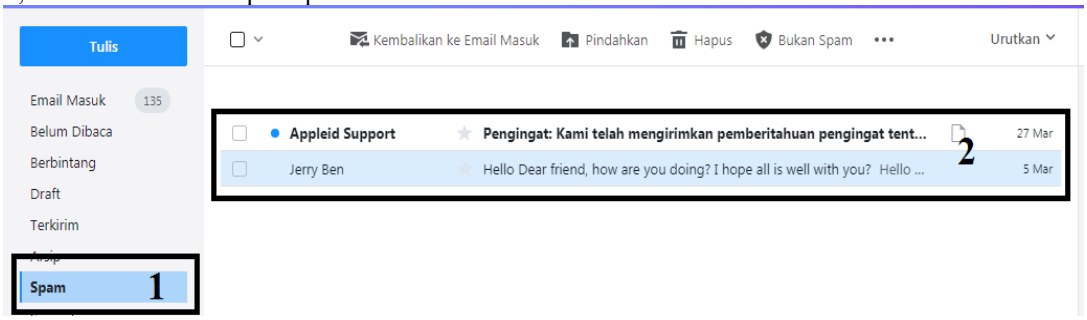

Figure 2. Inboxes in a spam folder

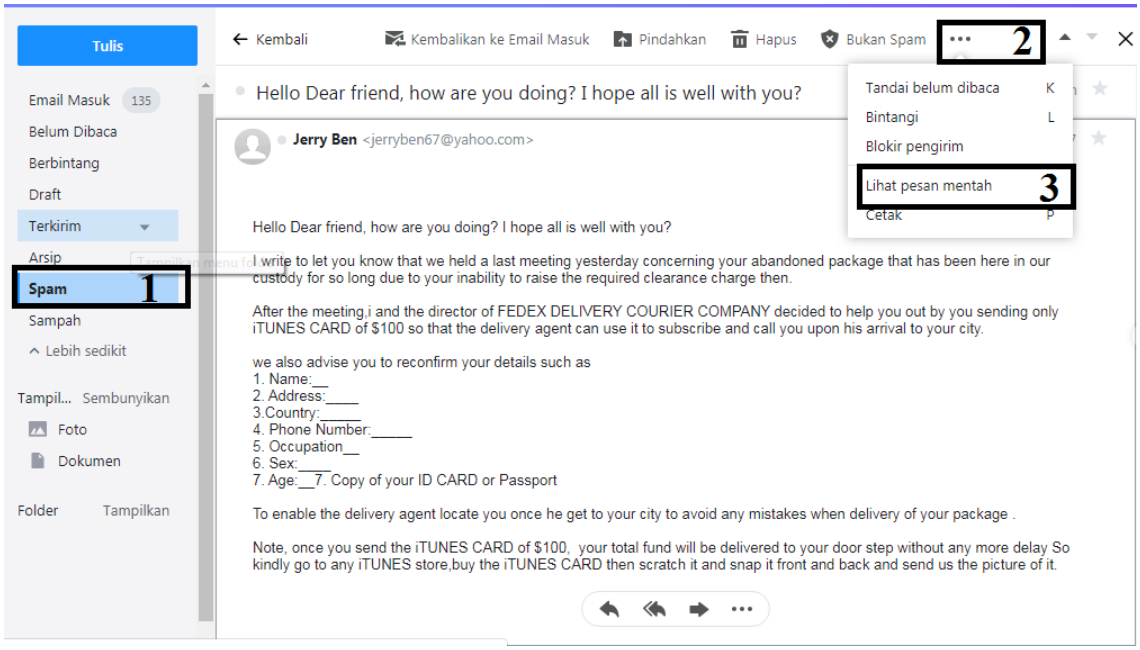

Figure 3. Spam Email Messages

Figure 2 and **Figure 3** shows the content of an email message located in the spam folder. To view the header of a spam email, click on the option and then click on View raw message.

B. Examination

The examination was run to determine data filtering in certain parts of the data source. Data filtering was carried out by changing the shape of the data but we did not make changes to the data content because the authenticity of the data was very important.

```
Return-Path: <jerryben67@yahoo.com>
X-YahooFilteredBulk: 74.6.134.215
Received-SPF: pass (domain of yahoo.com designates 74.6.134.215 as permitted sender)
X-YMailISG: C5vN1b8WLDs8JRY.tJIcucDYcONe.xKX5_poqOFVfQk5D0xN
 QJnB.cjiJZqtBA1YAUM3R1k99_KpRgjaynJOAH9xEy52HwxlswZYntVMVGxu
 W4vFOj2fQNUnHArknokjAa39eRHLcMmRGG8Z0hspswT4iZSqxJR9YgiZ6GK8
 0kC5N5xEaQjR11YU6gn0RfffvKTmaJhyK041aKoKOxxPWFIxwvpnS4jbjapU
 c_uIj78UoRurozZiW37isp1tzRO1ywiWPUvtYvH.tgNa_jNbjXC1W9n0ynRL
 U5GiYanyLvSKgJm1FmRcf2PJpbAWdTcFHRz72d3.wbOrDtqfnwKst1zBnxpS
 _laBr7cOgfu4cF1D9nLZfN4I1bIRasBM8Ta6ZUr4McNF1_K8cTjVYnr4BDiN
 XYjgLkY_1TVPriUKtPdXsxHA0A3bKHTC6lyBSfR98Uu9wuUrGPrzCwCvP1xG
 RTNp0CvC0UkES1Cp7erGmLr.1H8h.iXEJBMqKtGk8B9K7fAnYUtCrb3syEAE
 WZzpyeSFt1M3Z965XwweKrSedTDxQ5G_6BiWiS8NCFuYizeyaX4tK6GvyRHv
 Nm2GiMu5bw3cH3oWwKOZwVhnReIjSOB03SDLRNtgCewd7.4hj91Y_6PkZFG4
 baJuzQGUCs9X_dGf9fKtyDBJ7KNSSkkpsXs67eOEpnTLkr558f6gIMSLI6pu
 W2IzkoZUEUJbAikKsEtMxoT8dGBV8eoXs3BTeEBVQyhOV2wLwcueUXa5axki
 d9KVUVrUqu44Cun4LLL_Dx4WNHEypoEnRar0i29LuEV5Yj.rEUq1Zd4XoMPm
 VxM1rHCFzeyvdikKBIVuyKUPTiGQS0aud7jOgELqdcwNmHEVxFwXwBAZmrV8
 VIxIXKxCV9GnGUb7FPiUOdjrClhMeqQWaAhuAwM1dTUiiIpRHQEKsDsXHgZb
 blxoD0e1R3c.KjQXUtoga.1DEU4sgbUr11KsI6Ly8DQpwxVWERrFyI7vqsO3
 JAyfCQO5VgZMD7vDDRYm6SZYRbOzGEN_raBrLArJHgDdQK1MpVxG9qz9tSH0
 VhMgh63pag0WPS6POIct4lLn1KkeMafapaDQXR5LQcGtZ2Se6tE3Vo23ZDcB
 ZF8IjH9G6X5hS2JJkCulVURG2wMtJfJF4NVFrW0csHQhWE8zoPrCqYT01YZU
 INzIdY2Da.zNdg--
X-Originating-IP: [74.6.134.215]
Authentication-Results: mta4108.mail.sg3.yahoo.com
 header.i=@yahoo.com; header.s=s2048; dkim=pass (ok)
Received: from 127.0.0.1  (EHLO sonic315-41.consmr.mail.bf2.yahoo.com) (74.6.134.215)
  by mta4108.mail.sg3.yahoo.com with SMTPS; Mon, 04 Mar 2019 22:37:53 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1551739058; bh=Qw8CeErqGR1HT4h2qGsTSRoAMKTdAox7OgA2cfD331Q=; h=Date:Fror
b=HHK7EodRQQmP24YLg45GH6u0ZTFJWHmW4F5zg5rfPXJTT12FCPvNFfIAuNnEWE7k1RIINuoPm/ZofMyNXUcnRZ+w+c84MEhnENy7QFhZRPtchStmEIABCxsgp+sSXcXG0L8DjVQAxFY45DS7x1k\
ZOhe4dOetIJCyNs9VYhU0P/4yNargaOnn1hKccdAZ6K+jdmSBnJSzNQkrTZ3fLaNlbzJX/n8jrzcWarxVhCyi/zjIN8TSEdt8kEosvWdXC9XV6zeZFOrk6RaOFpLhUhybeUvedru5g==
X-YMail-OSG: fU5vpe0VM1nZ1u.sTe7em75Jg8vvIWtIFVpn7KOX9VtAEDBJK9IiS8JpniNdHA-
 -
Received: from sonic.gate.mail.ne1.yahoo.com by sonic315.consmr.mail.bf2.yahoo.com with HTTP; Mon, 4 Mar 2019 22:37:38 +0000
Date: Mon, 4 Mar 2019 22:35:36 +0000 (UTC)
From: Jerry Ben <jerryben67@yahoo.com>
Reply-To: Jerry Ben <officebank21@gmail.com>
Message-ID: <1413985146.9278424.1551738936539@mail.yahoo.com>
Subject: Hello Dear friend, how are you doing? I hope all is well with you?
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit
References: <1413985146.9278424.1551738936539.ref@mail.yahoo.com>
X-Mailer: WebService/1.1.13123 YahooMailBasic Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.119 Safari/537.36
Content-Length: 1072
```

Figure 4. Spam Email Headers

In **Figure 4** is a display of spam email headers. This email header was used for analysis of emails that entered the spam folder.

C. Analysis

The step taken was to analyze the generated. We analyzed where, how and why the data was generated, and by whom.

Header

X-Apparently-To:	Mon, 04 Mar 2019 22:37:53 +0000
Return-Path:	<jerryben67@yahoo.com>
X-YahooFilteredBulk:	74.6.134.215
Received-SPF:	pass (domain of yahoo.com designates 74.6.134.215 as permitted sender)
X-YMailISG:	C5vN1b8WLDs8JRY.tJIcucDYcONe.xKX5_poqOFVfQk5D0xN QJnB.cjiJZqtBA1YAUM3R1k99_KpRgjaynJOAH _laBr7cOgfu4cFlD9nLZfN4I1bIRasBM8Ta6ZUr4McNF1_K8cTjVYnr4BDiN XYjgLkY_lTVPriUKtPdXsxHA0A3bK baJuzQGUCs9X_dGf9fKtyDBJ7KNSSkkpsXs67eOEpnTLkr558f6gIMSLI6pu W2IzkoZUEUJbAikKsEtMxoT8dGI blxoD0e1R3c.KjQXUtoga.lDEU4sgbUrl1KsI6Ly8DQpwxVWERrFyI7vqsO3 JAyfCQO5VgZMD7vDDRYm6SZYR
X-Originating-IP:	[74.6.134.215]
Authentication-Results:	mta4108.mail.sg3.yahoo.com header.i=@yahoo.com; header.s=s2048; dkim=pass (ok)
Received:	from 127.0.0.1 (EHLO sonic315-41.consmr.mail.bf2.yahoo.com) (74.6.134.215) by mta4108.mail.sg3.yal
DKIM-Signature:	v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1551739058; bh=QW8CeErqGR1HT b=HHK7EodRQQmP24YLg45GH6u0ZTFJWHmW4F5zg5rfPXJTT12FCPvNFfIAuNnEWE7klRIINuoPm/ZofMyNX
X-YMail-OSG:	fU5vpe0VM1nZ1u.sTe7em75Jg8vvIWtIFVpn7KOX9VtAEDBJK9IiS8JpniNdHA- -
Received:	from sonic.gate.mail.ne1.yahoo.com by sonic315.consmr.mail.bf2.yahoo.com with HTTP; Mon, 4 Mar 201
Date:	Mon, 4 Mar 2019 22:35:36 +0000 (UTC)
Date (Formatted):	03/04/2019 22:35:36 UTC
From:	Jerry Ben <jerryben67@yahoo.com>
Reply-To:	Jerry Ben <officebank21@gmail.com>
Message-ID:	<1413985146.9278424.1551738936539@mail.yahoo.com>
Subject:	Hello Dear friend, how are you doing? I hope all is well with you?
MIME-Version:	1.0
Content-Type:	text/plain; charset=UTF-8
Content-Transfer-Encoding:	7bit
References:	<1413985146.9278424.1551738936539.ref@mail.yahoo.com>
X-Mailer:	WebService/1.1.13123 YahooMailBasic Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like G
Content-Length:	1072

Figure 5. Spam Email Header Details

Figure 5 describes the email sent by <jerry67@yahoo.com>, with the IP (X-Originating-IP :74.6.134.215). From the analysis of the spam email headers, we could trace where it came from, but we did not know yet who did it because only the IP Address was recorded (74.6.134.215). IP address trace results show in **Figure 6**.

There were 5 IP address administrators in the world. These five administrators are those who regulate the use of IP addresses on every computer in the world. The five administrator ip addresses are:

1) ARIN (North America and Sub-Sharan Africa) website: www.arin.net.
2) RIPE (Europe and Northern Africa) website: www.ripe.net.
3) APNIC (Asia Pacific) website: www.apnic.net.
4) LACNIC (Southern and Central America and the Caribbean) website : www.lacnic.net.
5) AFRINIC (The African Network Information Centre) website: www.afrinic.net.

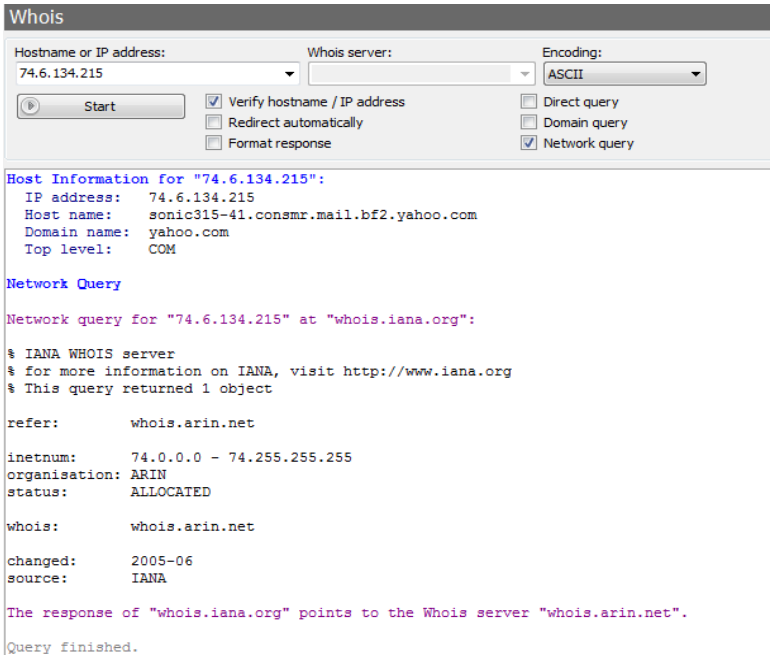

Figure 6. IP address trace results

After analyzing the IP of the spam email sender, the eToolz application notified that the IP (74.6.134.215) belonged to ARIN.

D. Reporting

At these digital forensics reporting stage, from the 3 stages that we run, digital forensic evidence was obtained. At the previous stage, we managed to get digital evidence in the form of an IP address contained in the email header.

Conclusion

Based on the results of the tests conducted using the NIST method, it can be concluded that e-mail header investigation was an important aspect of the investigation because e-mail metadata and other information were contained the in e-mail headers. Analysis of e-mail headers could reveal the source, destination, e-mail client, sender IP, identification of fake or authentic e-mails, and more. IP addresses could be tracked using applications to make it easier to find the sender of the e-mail. Once an IP address was tracked, it was easy to find routes, geographic locations, network providers, and more.

Based on the results of the research, the authors suggest that hopefully the current study can be useful for developing better tools so that it can be more effective and the results obtained are more detailed. More previous studies reviews are needed so that the research results are more accurate and digital evidence can be used as evidence.

References

[1] Nasiroh, S., 2019, Analisis Digital Forensic Readiness Index (DiFRI) sebagai Tindakan Preventif Cybercrime, Tesis, Magister Teknik Informatika UII:Yogyakarta.
[2] Devendran, V.K., Shahriar, H., and Clincy, V., A Comparative Study of E-mail Forensic Tools, Journal of Information Security Vol., 111-117, 2015.
[3] Chhabra, G. S, Review of E-mail System, Security Protocols and Email Forensics, 5(3), 201–211, 2015.
[4] Saidi, L.A.O., 2017, Pengembangan Framework untuk Investigasi E-mail Forensics menggunakan Metode System Development Life Cycle (SDLC), Tesis, Magister Teknik Infoematika UII:Yogyakarta.
[5] Hayuningtyas, R.Y., Aplikasi Filtering of Spam E-mail Menggunakan Naïve Bayes. IJCIT (Indonesian Journal on Computer and Information Technology) Vol.2 No.1, pp. 53-60, 2017.
[6] Hatole, P.P dan Bawiskar, S.K. Literature Review of E-mail Forensics. Imperial Journal of Interdisciplinary Research (IJIR) Vol-3, Issue-4, 2017
[7] Changhee, C., Hwaseong, L, Ilhoon J, Changon, Y dan Hosang Y. 2017. E-mail Header Analysis for Author Identification. 6th International Symposium on the Fusion of Science and Technologies (ISFT2017) Jeju, S. KOREA 17th
[8] Fadlil, A., Riadi, I., dan Aji, S., Pengembangan Sistem Pengamanan Jaringan Komputer Berdasarkan Analisis Forensik Jaringan, Jurnal Ilmu Teknik Elektro Komputer dan Informatika (JITEKI)Vol.3, No.1 hal.11-19, 2017.
[9] Umar, R., Yudhana, A., dan Faiz, M.N., Analisis Kenerja Metode Live Forensics untuk Investigasi Random Access Memory pada Sistem Proprietary, dalam Prosiding Konferensi Nasional Ke-4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM), pp. 207-211, 2016.
[10] Riadi, I., Eko, J., Ashari, A., dan Sunardi, Internet Forensics Framework Based-on Clustering International Journal of Advanced Computer Science and Applications, Vol.4 No.12 Hal.115-123. 2016.
[11] M. I. Mazdadi, I. Riadi, dan A. Luthfi, "Live Forensics on RouterOS using API Services to Investigate Network Attacks," Int. J. Comput. Sci. Inf. Secur., vol. 15, pp. 406–410, 2017.
[12] I. Riadi, R. Umar, dan A. Firdonsyah, "Identification of Digital Evidence on Android' s," vol. 15, no. 5, pp. 3–8, 2017
[13] Wijaya, H., Riadi, I., dan Sunardi, Analisis Forensik Digital Aplikasi Telegram pada Smartphone Berbasis Android, Seminar Nasional Teknologi Informasi dan Komunikasi (SEMANTIKOM) Hal 93-95, 2017
[14] Yudhana, A., Riadi, I., dan Anshori, I., Analisis Bukti Digital Facebook Messenger Menggukan Metode NIST, IT Journal Reserch and Development Vol. 3 No. 1, Hal 13-21. 2018
[15] Hoiriyah, Sugiantoro, B., dan Prayudi, Y., Investigasi Forensik pada email Spoofing menggukan Metode Header Analysis, Jurnal Ilmiah Dasi, Vol. 17 No 4 Hal 20-25, 2016.
[16] M. I. Syahib, I. Riadi, and R. Umar, "Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST)," J-SAKTI (Jurnal Sains Komput. dan Inform., vol. 4, no. 1, p. 170, 2020.