JISKA (Jurnal Informatika Sunan Kalijaga)
Vol. 7, No. 2, MEI, 2022, Pp. 83 – 90
ISSN: 2527 – 5836 (print) | 2528 – 0074 (online)

Analisis Forensik pada *Email* Menggunakan Metode *National Institute of Standards Technology*

Imam Riadi [(1)], Sunardi [(2)], Fitriyani Tella [(3)*]
[1] Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan, Yogyakarta
[2] Teknik Elektro, Fakultas Teknik Industri, Universitas Ahmad Dahlan, Yogyakarta
[3] Magister Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
e-mail : imam.riadi@is.uad.ac.id, sunardi@mti.uad.ac.id,
fitriyani1907048012@webmail.uad.ac.id.
* Penulis korespondensi.
Artikel ini diajukan 25 Agustus 2021, direvisi 9 November 2021, diterima 9 November 2021, dan dipublikasikan 25 Mei 2022.

Abstract

Nowadays developments in information technology are growing rapidly, especially in email. Email became one that almost the whole world had. Email is one of the results of developments in information and communication. Email is widely used to exchange information by sending and receiving data, such as document files, pictures, letters, and others. So much for the crimes that often occur in emails. Email crimes that often occur among them are email spoofing. Email spoofing is a forgery that occurs in the header of the email. So, the email is sent as if it were a valid email. Email spoofing is often used in spamming activities. Crimes committed by cybercrime must leave evidence such as IP Address, sender's email, and time of sending the email. This research will do forensics on email spoofing. The research uses the Live Forensics method, where the computer is used in a powered-on state. The research also uses the NIST (National Institute of Standards Technology) research flow. The email that will be analyzed is in the email header section using 3 tools, namely tracer email analyzer, email dossier, and mail header analysis. This analysis will compare and check the accuracy of the email headers using these tools. Emails suspected of email spoofing will be proven using tools. Based on the 'form' received' and 'Message-ID' headers. Based on the results, the tool that meets the value after the analysis is tracer email analysis.

Keywords: Email Spoofing, Header Email, Live Forensics, NIST, Three Tools

Abstrak

Saat ini perkembangan teknologi informasi berkembang pesat terutama pada *email. Email* menjadi salah satu yang hampir seluruh dunia memilikinya. *Email* merupakan salah satu hasil dari perkembangan dalam informasi dan komunikasi. *Email* banyak digunakan untuk bertukar informasi dengan mengirim dan menerima data, seperti file dokumen, gambar, surat dan lain-lain. Sehingga banyak menimbulkan kejahatan yang terjadi pada *email*. Kejahatan *email* yang sering terjadi yaitu *email spoofing*. *Email spoofing* merupakan pemalsuan yang terjadi pada bagian *header email*. Sehingga *email* yang dikirim seolah-olah berasal adalah *email* yang *valid*. *Email spoofing* sering digunakan dalam aktivitas *spamming.* Kejahatan yang dilakukan oleh *cyber-crime* pasti meninggalkan barang bukti seperti *IP Address,* email pengirim maupun waktu pengiriman *email*. Penelitian ini akan melakukan *forensic* pada email *spoofing*. Penelitian menggunakan metode *Live Forensics*, di mana komputer digunakan dalam keadaan menyala. Penelitian juga menggunakan alur penelitian NIST (*National Institute of Standards Technology*). Email yang akan dianalisis yaitu pada bagian *header email* dengan menggunakan 3 *tools* yaitu *tracer email analyzer*, *email dossier* dan *mail header analysis*. Analisis ini akan membandingkan dan memeriksa keakuratan pada *header email* menggunakan *tools* tersebut. *Email* yang diduga *email* spoofing akan dibuktikan menggunakan *tools*. Berdasarkan *header 'form' received'* dan *'message-ID'.* Berdasarkan hasil yang dilakukan *tools* yang memenuhi *value* setelah dilakukan analisis adalah *tracer email analysis*.

Kata Kunci: *Email Spoofing, Header Email, Live Forensics,* NIST*,* Tiga *Tools*

1. PENDAHULUAN

Internet merupakan bagian dari perkembangan teknologi, internet memberikan banyak dampak perubahan besar bagi masyarakat. Sejak adanya covid-19 segala aktivitas manusia telah berganti menajdi aktivitas digital didunia internet mulai dari sekolah, perkantoran maupun yang lainnya (Putra, 2016). Salah satu yang banyak digunakan dunia adalah *email. Email* merupakan aplikasi yang sangat popular dan digunakan setiap hari untuk pribadi, bisnis atau untuk yang resmi (Chhabra & Bajwa, 2012).

Jumlah pengguna *email* yang meningkat tentu membawa dampak positif dan negatif pada dunia internet. Salah satu dampak negatif yang sering bermunculan adalah beberapa orang pengguna *emai*l melakukan kejahatan digital (Yudhana et al., 2018). Kemudahan *email* yang ditawarkan terdapat ancaman yang cukup serius yaitu dengan memanfaatkan *email* sebagai media untuk melakukan tindak kejahatan didunia *cyber* (Sutisna, 2018).

Salah satu kejahatan yang sering terjadi adalah *spoofing email*. *Spoofing* adalah *email* yang dipalsukan dan dikirim seolah-olah berasal dari sumber yang dapat dipercaya (Nadzifan et al., 2018). Para pelaku *spoofing* melakukan manipulasi data yang dilakukan pada *header email* untuk menyamar sebagai pengguna *email* yang sah. Laporan intelijen Symnatec melaporkan bahwa 68% dari semua *email* adalah spam, satu dari 358,2 *emai*l diidentifikasikan sebagai *email phishing* dan 274,0 email berisi *malware* (Mishra et al., 2012).

Email spoofing digunakan pelaku untuk menyembunyikan alamat *email* yang asli dengan mengubah beberapa *field* pada *email* seperti *"from", "return-path"* dan *"replay to"*. Sehingga *email* terlihat seperti *email* yang asli dan dapat mengelabui penerima yang kurang paham terhadap *email* dan terjebak dalam skenario yang telah dibuat oleh pelaku (Hoiriyah et al., 2016).

Penelitian ini bertujuan untuk menganalisa *email* yang diduga merupakan *email spoofing*. Mengumpulkan barang bukti dari *header email* yang mendukung proses analisis untuk melacak pelaku *spoofing*. *Header* akan menunjukkan email server asal, sehingga dibutuhkan penanganan forensik terhadap tindak kejahatan yang melibatkan *email* tersebut. Forensik dilakukan menggunakan *tools* forensik yaitu iptrackonline, domain dossier dan tracer email analyzer. Penelitian menggunakan satu studi kasus dan akan dianalisis menggunakan ketiga *tools* tersebut. Sehingga ditemukan keakuratan menemukan barang bukti berdasarkan hasil analisis dari *tools* forensik yang digunakan.

Digital forensik adalah ilmu yang mempelajari tentang cara untuk menangani berbagai kejahatan dalam dunia *cyber* (Kurniawan & Prayudi, 2014). Forensik digital adalah ilmu yang digunakan untuk mengumpulkan, memverifikasi, mengidentifikasi, menganalisis, menafsirkan, mendokumentasikan dan mempresentasikan bukti digital yang diperoleh dari sumber digital dengan tujuan membantu memprediksi perilaku yang menghambat jalannya analisis yang direncanakan (Rizal, 2018).

Forensik jaringan adalah kegiatan untuk merekam dan menganalisa peristiwa yang terjadi dalam jaringan untuk menemukan sumber serangan dan peristiwa lainnya (Fahana et al., 2017). Forensik jaringan berkaitan dengan perubahan data dan berakar dari keamanan jaringan dan deteksi penyusupan. Forensik komputer juga merupakan ilmu baru dalam bidang komputer sedangkan forensik jaringan merupakan ilmu yang dalam hal teknologi masih dalam tahap pertumbuhan (Putri & Istiyanto, 2013).

Email adalah sebuah metode untuk melakukan komunikasi untuk mengirimkan pesan dalam bentuk digital. *Email* terdiri dari dua bagian utama yaitu *header* dan *body email* (Nugroho et al., 2016). Pesan *email* dikirim melalui internet. Sebuah pesan yang mencakup isi, alamat pengirim dan alamat email yang akan dikirim. *Email* adalah satu-satunya aplikasi internet yang digunakan untuk semua pengguna internet (Nadzifan et al., 2018).

Live forensics adalah metode yang menyimpan hampir semua penggunaan sistem dalam RAM, *file paging*, *file* hibernasi dan *file crash dump*. Sehingga harus dijalankan dalam keadaan sistem belum mati (Yudhana et al., 2019).

2. METODE PENELITIAN

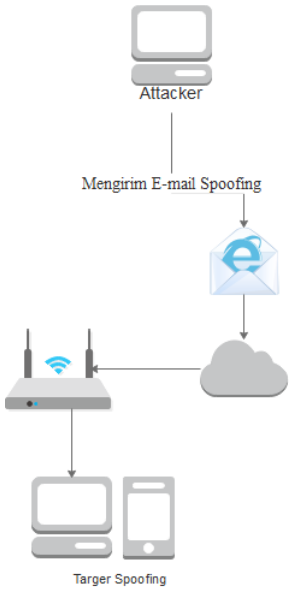
Metode penelitian yang digunakan untuk menganalisis bukti forensik pada *email* atau tahapan untuk mendapatkan informasi dari bukti digital adalah dengan metode NIST (*National Institute of Standars Technology*) (Yudhana et al., 2018). Langkah-langkah metode ini diimplementasikan dan dapat dilihat dalam proses penyelidikan secara terstruktur dan digunakan sebagai acuan untuk memecahkan masalah yang ada (Syahib et al., 2020). Adapun tahapan metode dapat dilihat pada Gambar 1.

Gambar 1 Metode NIST

Berdasarkan pada Gambar 1, pada tahap *collection* yaitu melakukan alur atau simulasi yang akan digunakan untuk analisis. Selain itu *tools* yang digunakan berkaitan dengan *email spoofing*. Tahap *examination* melakukan pengolahan data yang telah dikumpulkan secara forensik dengan menggunakan skenario atau simulasi yang dilakukan. Tahapan *analysis* melakukan hasil pemeriksaan dengan menggunakan *tools* forensik. Tahap *reporting* yaitu hasil analisis yang mencakup deskripsi tindakan forensik yang diambil (Anwar & Riadi, 2017). Jika langkah sebelumnya belum dilakukan atau gagal, maka langkah selanjutnya tidak dapat dilanjutkan. Metode ini akan membantu untuk mengembangkan kerangka kerja.

3. HASIL DAN PEMBAHASAN

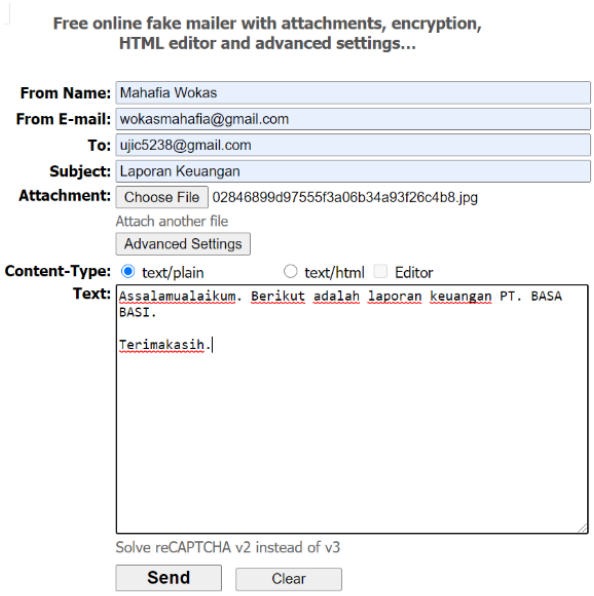
Pengoleksian barang bukti dalam penelitian ini menggunakan *tools* yaitu Email Dossier, Tracer Email Analyzer dan Iptrackonline. Proses pengambilan *email* dilakukan menggunakan simulasi sebagai serangan untuk melakukan *email spoofing*, seperti yang ditunjukkan pada Gambar 2.



Gambar 2 Alur Simulasi *Email Spoofing*

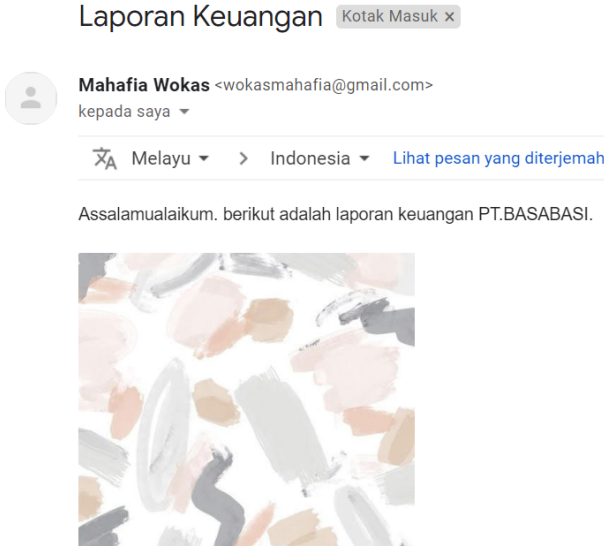
Pada Gambar 2 merupakan alur simulasi dari *email spoofing*. Hal pertama yang dilakukan adalah membuat *email* palsu dan mengirimkan kepada korban seolah-olah *email* yang dikirim berasal dari pemilik *email* yang asli. Setelah email diterima oleh korban, kemudian dari bukti *email* tersebut akan dilakukan analisis menggunakan ketiga *tools* tersebut.

Proses pengiriman *email* menggunakan tools *Emkei'z fake emails*. Pengirim *email* korban adalah wokasmahafia@gmail.com dan *email* pelaku yaitu ujic5238@gmail.com. *Email* yang dikirim berisikan laporan keuangan dari PT. BASA BASI, dapat dilihat pada Gambar 3.



Gambar 3 Pengiriman *Email Spoofing*

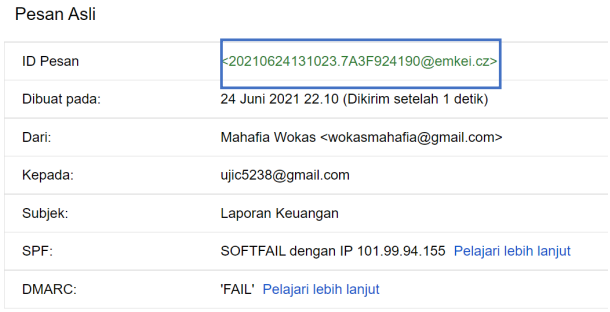
Proses pengiriman *email* yang pertama dilakukan adalah melakukan pengiriman *email* menggunakan *email* yang asli yaitu menggunakan situs resmi gmail.com. Selanjutnya menggunakan tools *Emkei'z fake emails* untuk pengiriman *email spoofing*. Sedangkan pada Gambar 4 dan 5 merupakan isi *field email* yang terima dari pelaku kepada korban.



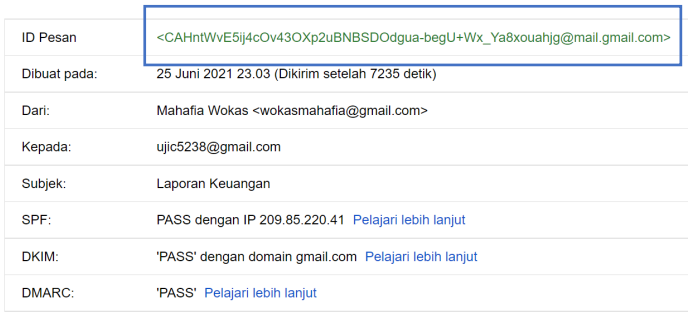
Gambar 4 *Field Email* yang Valid

Gambar 5 *Field Email Spoofing*

Jika diperhatikan pada Gambar 4 dan Gambar 5 hampir tidak perbedaan isi *field* antara kedua *email* tersebut. Isi *field* kedua *email* terlihat nampak identik. Namun jika dianalisis Kembali, *email* tersebut terdapat perbedaan yang datang dari orang yang mengirimkan *email* atau dari alamat *email* yang berbeda ataupun tempat yang berbeda. Bukti lainnya dapat dilihat dari *header* kedua *email* tersebut.



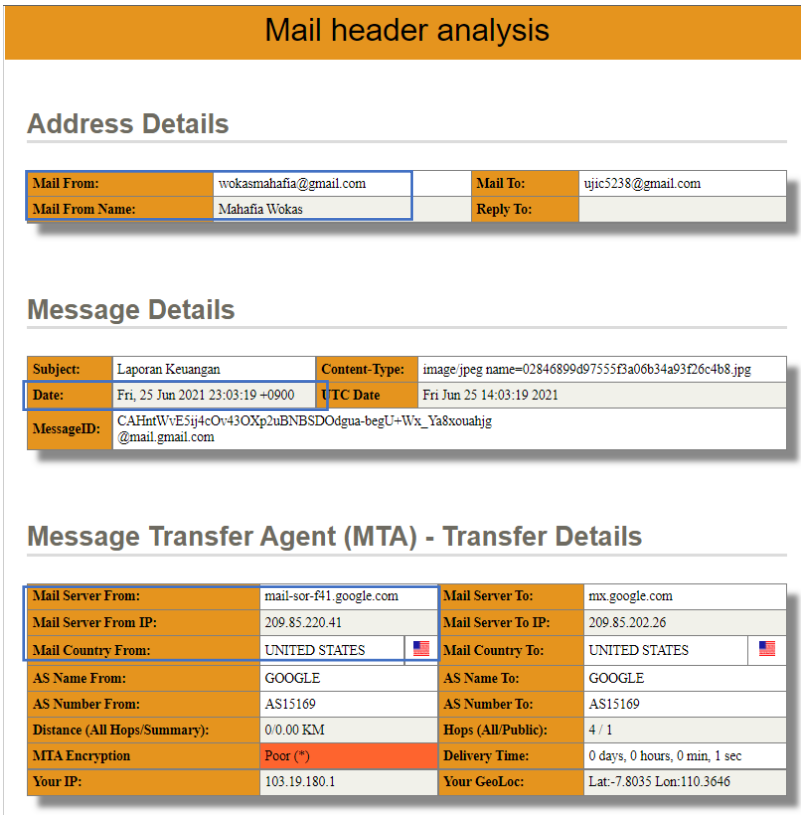
Gambar 6 *Header Email Spoofing*



Gambar 7 *Header Email* Asli

Merujuk pada Gambar 6 email *spoofing* yang dikirimkan oleh pelaku pada ID pesan *spoofing* tersebut dikirimkan melalui *emkei'z fake emails* bukan dari Gmail. Sedangkan pada Gambar 7, email tersebut merupakan *email* asli yang dikirimkan langsung melalui situs Gmail. Maka dapat diidentifikasikan bahwa *email* yang diterima merupakan *email spoofing*.

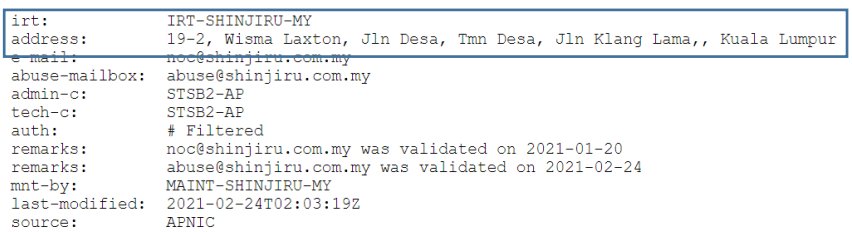
Selanjutnya akan dilakukan pengujian terhadap *email spoofing* tersebut. Analisis pertama yang dilakukan menggunakan *tools mail header analysis* seperti pada Gambar 8.



Gambar 8 Hasil Menggunakan *Mail Header Analysis*

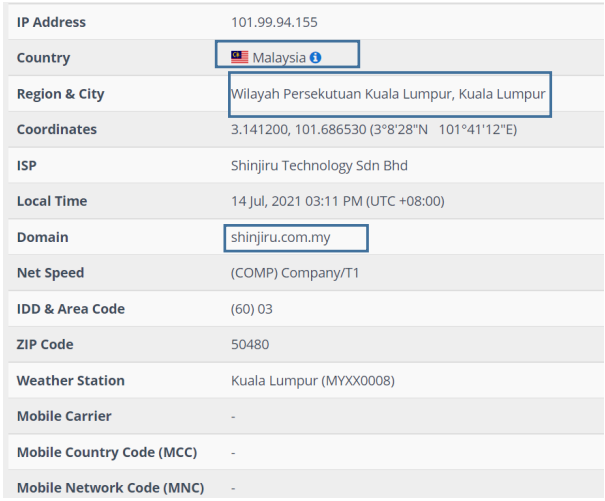
Pada Gambar 8 hasil pengujian menunjukkan bahwa *tools mail header analysis* dapat menampilkan informasi dari *header email* berupa *email* pengirim dan penerima, subjek dari *email*, tanggal pengiriman *email* dan alamat IP dari *server* pengirim *email* dan lokasinya. Selain itu juga ditampilkan informasi *MessageID* dari *email* yang dikirimkan, nama *server* pengirim dan penerima *email*, dan lama waktu pengiriman. Terlihat bahwa *email* dikirimkan dari alamat ujic5238@gmail.com kepada wokasmahafia@gmail.com dengan subjek “Laporan keuangan”. *Email* dikirimkan pada 25 Juni 2021 jam 23:03 WIB.

Selanjutnya analisis menggunakan *tools* kedua yaitu *email dossier*. Cara kerja dari *tools* ini yaitu dengan memasukkan IP yang akan diuji. Pengujian menggunakan *email dossier* ditemukan adanya *IP address* pengirim dan nama *server*. Menunjukkkan daerah dan negara email tersebut dikirim diantaranya menunjukkan *address* pengirim, email pengirim dan admin. Dilihat pada Gambar 9.



Gambar 9 Hasil Menggunakan *Email Doisser*

Pengujian menggunakan *tracer email*. Hasil pengujan menunjukkan *email* yang masuk berasal dari Malaysia dan dengan nama perusahaan yang sama seperti pengujian *tools* sebelumnya. Hasil pengujian dapat dilihat pada Gambar 10.



Gambar 10 Hasil Menggunakan *Tracer Email Analyzer*

Berdasarkan dari ketiga *tools* yang digunakan dan telah dilakukan analisis terhadap *email spoofing*. Maka dapat diketahui perbedaan hasil dari *tools* yang telah digunakan pada Tabel 1.

Tabel 1 Hasil Perbandingan *Tools*

Analisa	*Tracer email analyzer*	*Email dossier*	*Mail header analysis*
Server email	√	√	√
Message-Id	√	√	√
Received Form	√	√	-
Received From user	√	-	√
source IP address	√	√	√
Host Address	√	-	√
Data sent	√	√	√
Country	√	-	√
Browser sent email	√	-	-
Host name	√	√	√

Berdasarkan Tabel 1 yang menjelaskan hasil dari email *spoofing* berdasarkan *tools forensics* yang digunakan yaitu *tracer email analyzer, mail header analysis* dan *email dossier*. Ketiga *tools* tersebut menjelaskan proses analisis pada *email spoofing* dapat dibuktikan dari mana *email* tersebut dikirim, *IP address* pengirim, alamat, *domain email*. Sehingga menunjukkan bahwa tingkatan analisis yang sangat baik adalah *tracer email analyzer*. Sehingga dikatakan bahwa *email* yang telah dianalisis adalah benar merupakan *spoofing email*.

Dikatakan *tools tracer email analyzer* lebih baik karena berdasarkan hasil analisis untuk mendapatkan barang bukti dengan menggunakan *Email tracer analyzer*. *Email tracer analyzer* dapat menemukan informasi yang dapat dijadikan barang bukti, diantaranya adalah domain pelaku yaitu *email* dari mana dan IP *address* si pengirim, *email* yang dikirim telah melalui beberapa *email address* yang lain, subjek *email,* Tanggal *email* dikirim dan diterima dan *web browser email*. Sedangkan pada *email dossier* hanya ditemukan informasi berupa barang bukti diantaranya *ip address* pengirim dan nama *server*nya, daerah atau negara *email* berasal dan IP *address* pengirim, *email* pengirim dan admin. *Mail header analysis* hanya ditemukan barang bukti berupa *email* pengirim dan penerima, subjek dari *email*, tanggal pengiriman *email* dan alamat IP dari *server* pengirim *email* dan lokasinya.

4. KESIMPULAN

Berdasarkan hasil pengujian dan analisis yang dilakukan untuk mengetahui ciri-ciri dari *email spoofing*. *Email* yang mudah dipalsukan adalah pada bagian *header email*. Penelitian dengan menggunakan metode *live forensics* dan NIST, dimana komputer tetap dalam keadaan menyala. Analisis yang dilakukan adalah pada bagian *header email* yang rinci pada *email* yang diterima. Proses pengujian menggunakan *tools forensics* berjalan dengan baik. *Tools* yang digunakan adalah *mail header analysis, email dossier* dan *tracer email analyzer*. *Tools* yang digunakan menghasilkan barang bukti *email spoofing* yang telah melewati pengujian dengan *value tools* yang sangat baik adalah *tracer email analyzer*. Dari hasil penelitian tersebut, dapat dijadikan barang bukti sehingga perlu dilakukan analisis lebih jauh sehingga perlu dilakukan analisis lebih jauh agar mendapatkan hasil barang bukti forensik yang lebih relevan.

DAFTAR PUSTAKA

Anwar, N., & Riadi, I. (2017). Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *3*(1), 1. https://doi.org/10.26555/jiteki.v3i1.6643

Chhabra, G. S., & Bajwa, D. S. (2012). Review of E-mail System, Security Protocols and Email Forensics. *International Journal of Computer Science & Communication Networks, 5*(3), 201–211.

Fahana, J., Umar, R., & Ridho, F. (2017). Pemanfaatan Telegram sebagai Notifikasi Serangan untuk Jaringan Forensik. *QUERY: Jurnal Sistem Informasi*, *1*(2), 6–14.

Hoiriyah, Sugiantoro, B., & Prayudi, Y. (2016). Investigasi Forensik Pada Email Spoofing Menggunakan Metode Header Analysis. *Jurnal DASI*, *17*(4), 20–25.

Kurniawan, A., & Prayudi, Y. (2014). Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics. *HADFEX (Hacking and Digital Forensics Exposed)*, 1–5.

Mishra, P., Pilli, E. S., & Joshi, R. C. (2012). Forensic Analysis of E-mail Date and Time Spoofing. *2012 Third International Conference on Computer and Communication Technology*, *November*, 309–314. https://doi.org/10.1109/ICCCT.2012.69

Nadzifan, A. M., Nazihullah, F., & . S. . (2018). Aplikasi untuk Deteksi Adanya Spoof pada Email. *SISTEMASI*, *7*(3), 268. https://doi.org/10.32520/stmsi.v7i3.380

Nugroho, N. B., Azmi, Z., & Arif, S. N. (2016). Aplikasi Keamanan Email Menggunakan Algoritma RC4. *Jurnal SAINTIKOM*, *15*(3), 81–88.

Putra, E. N. (2016). Pengiriman E-Mail Spam Sebagai Kejahatan Cyber di Indonesia. *Jurnal Cakrawala Hukum*, *7*(2), 169–182. https://doi.org/10.26905/idjch.v7i2.1906

Putri, R. U., & Istiyanto, J. E. (2013). Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *7*(1), 101–112. https://doi.org/10.22146/ijccs.2157

Rizal, R. (2018). *Network Forensics untuk Mendeteksi Serangan Flooding pada Perangkat Internet of Things (IoT)*. Universitas Islam Indonesia.

Sutisna, M. A. (2018). Analisa Forensik pada email spoofing. *Jurnal Teknologi Terpadu*, *4*(1), 38–43. https://doi.org/10.54914/jtt.v4i1.104

Syahib, M. I., Riadi, I., & Umar, R. (2020). Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST). *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, *4*(1), 170. https://doi.org/10.30645/j-sakti.v4i1.196

Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. *IT Journal Research and Development*, *3*(1), 13–21. https://doi.org/10.25299/itjrd.2018.vol3(1).1658

Yudhana, A., Riadi, I., & Zuhriyanto, I. (2019). Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS). *TECHNO*, *20*(2), 125–130. https://doi.org/10.30595/techno.v20i2.4594