JURNAL ILMIAH FIFO **P-ISSN 2085-4315 / E-ISSN 2502-8332**
DOI: http://dx.doi.org/10.22441/fifo.2020.v12i2.001

Perbandingan Hasil Forensics Jaringan Terhadap Serangan E-mail Spamming dan Spoofing

Fitriyani Tella[1], Imam Riadi[2], Sunardi[3]

[1]*Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan*
[2]*Program Studi Sistem Informasi, Universitas Ahmad Dahlan*
[3]*Program Studi Teknik Elektro, Universitas Ahmad Dahlan*
Kampus III UAD Jl. Prof. Dr. Soepomo, Janturan, Umbulharjo, Yogyakarta
[1]fitriyani1907048012@webmail.uad.ac.id, [2]imam.riadi@is.ac.id, [3]sunardi@mti.ac.id

Abstract

In the era of technology, email has become one of the important things in the means of communication. Email is a medium for communication and also a place to store crime. One common crime is email spamming and spoofing. Spam is junk mail or unwanted messages, this spam email will be sent to someone's inbox and is useless to the recipient. Spam is sent on the network to increase network traffic. Email spoofing is a way to hide the origin of messages used by spammers. Email spoofing can change the email sender's information ie in the "From" field. Email spoofing comes from the sender which will make the email look like the real sender. The technique used to determine the comparison of email spoofing and spamming attacks using a method is the Network Forensics Development Life Cycle (NFDLC). Network forensics is performed to find out the IP address of the spamming and spoofing e-mail attacks. This research will also produce an email forgery pattern in the header, place and date of the perpetrators of the crime attacks.
Keyword: articles, english, Abstracts

Abstrak

Pada Era teknologi sekarang email telah menjadi salah satu hal yang penting dalam sarana komunikasi. Email merupakan salah satu media untuk berkomunikasi dan juga menjadi tempat untuk menyimpan kejahatan. Salah satu kejahatan yang sering terjadi adalah email spamming dan spoofing. Spam adalah junk mail atau pesan yang tidak diinginkan, spam email ini akan dikirimkan kepada inbox mail seseorang dan tidak berguna untuk penerima. Spam dikirim pada jaringan untuk meningkatkan lalu lintas jaringan. Email spoofing adalah cara untuk menyembunyikan asal usul pesan yang digunakan oleh spammer. Email spoofing dapat mengubah informasi pengirim email yaitu pada bidang "From". Email spoofing berasal dari pengirim yang akan menjadikan email tampak seperti pengirim sebenarnya. Teknik yang dilakukan untuk mengetahui perbandingan dari serangan email spoofing dan spamming yaitu menggunakan metode adalah Network Forensics Development Life Cycle (NFDLC). Dilakukan forensik jaringan guna mengetahui ip address dari serangan email spamming dan spoofing tersebut. Penelitian ini juga akan menghasilkan pola pemalsuan email pada header, tempat dan tanggal dari pelaku melakukan serangan kejahatan.
Keyword: *Forensik Jaringan, E-mail Spamming, E-mail Spoofing*

I. Pendahuluan

Layanan internet yang digunakan untuk membantu manusia melakukan aktivitasnya dimanapun. Pertumbuhan penggunaan internet berkembang didunia. Pertukaran informasi saat ini telah banyak yang menggunakannya, salah satunya penggunaan *e-mail (electronik mail*). Ilmu forensik merupakan ilmu yang bisa dikatakan baru dan bahkan belum banyak dikenal atau diketahui dikalangan masyarakat. Kejahatan didunia

cybercrime memiliki banyak variasi berbeda dengan dunia maya, salah satunya adalah pemalsuan atau spam email [1]. Forensik jaringan yang lebih spesifik adalah kegiatan menangkap, menganalisa, dan mencatat kejadian segala jaringan komputer untuk menemukan sumber serangan keamanan atau masalah kejadian lainnya. Kekuatan dari forensik adalah memungknkan analisis dan mendapatkan kembali kejadian ataupun fakta, karena fakta mungkin saja tersembunyi [2]

E-mail merupakan salah satu fasilitas untuk mengirimkan surat berbasis digital dan sangat berperan penting dalam sebuh institusi atau lembaga untuk melakukan komunikasi dan bertukar informasi. Sehingga *e-mail* dapat disalah gunakan untuk mendapatkan informasi dengan cara mengubah identitas pengirim dan menjadikannya seperti berasal dari pengguna *e-mail* yang asli merupakan istilah dari *e-mail spoofing* [3]. Spam pesan *e-mail* adalah pesan *e-mail* massal yang tidak diinginkan, sering dikirim ke banyak orang dengan sedikit atau tidak ada perubahan dalam konten [4].

Permasalahan diatas akan dilakukan penelitian untuk membedakan berupa *e-mail spoofing* dan *spamming*. Penelitian ini menggunakan metode NFDCL (*Network Forensics Development Life Cycle)* dengan pendekatan forensik jaringan yang menghasilkan pemalsuan email yang berupa subjek, alamat dan tanggal *e-mail*. Selain itu *e-mail* forensik menghasilkan forensik jaringan dengan mengetahui *ip address* pengguna kejahatan.

Penelitian sebelumnya yang dilakukan oleh [5] melakukan penelitian dengan membandingkan keamanan email berdasarkan browser yang digunakan. Peneliti menggunakan browser secara umum sepertu *Google chrome. Mozilla Firefix,* dan *Microsoft Edge.* Studi kasus peneliti berfokus pada keamanan beberapa *E-mail* seperti *Gmail, Yahoo,* dan *outlook.* Hasil dari penelitian ini penyedia *e-mail* dapat menambahkan fitur tersendiri demi keamanan *user.*

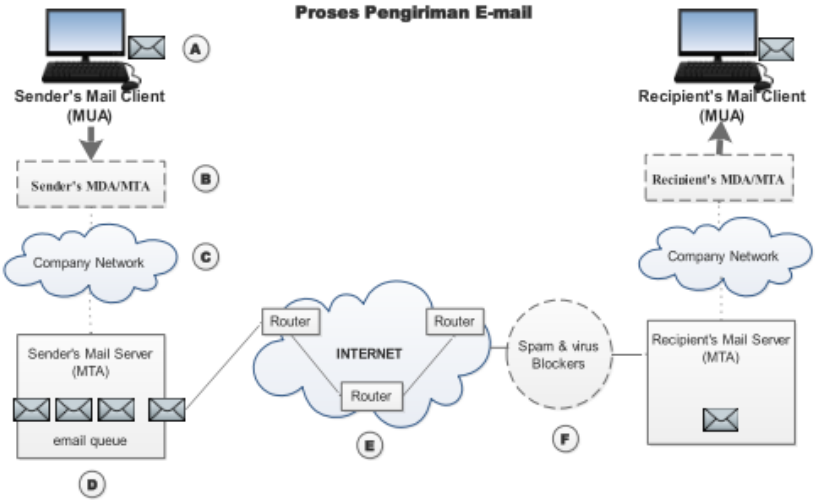
Penelitian yang dilakukan oleh [6] melakukan penelitian terhadap serangan *e-mail spoofing* dengan melakukan analysis pada *header e-mail* yang diterima dengan menggunakan metode pada penelitian adalah DFRWS (*Digital Forensics Research Workshop*). Hasil dari penelitian ini adalah dengan memanfaatkan layanan web *hosting e-mail spoofing* dapat dikirimkan. Pengiriman *e-mail* dengan layanan web hosting menggunakan pemrograman PHP. Penelitian menghasilkan perbedaan antara *e-mail* asli dan *e-mail spoofing*

Penelitian yang dilakukan [7] melakukan penelitian tentang pendekayan investigasi dan tools yang memiliki kelebihan dan kekurangan masing-masing, sehingga pengguna dapat menyesuaikan dengan kebutuhan.

Forensik Jaringan (*Network Forensics*) adalah menganalisis sebuah kejadian pada jaringan dengan kegiatan menganalisis, menangkap dan mencatat untuk menemukan keamanan atau masalah dan menemukan sumber serangan kejadian lainnya. Kekuatan dari forensik adalah mendapatkan kembali fakta dari kejadian yang terjadi dan menemukan kembali fakta yang mungkin saja tersembunyi [8].

Electronic Mail atau dapat disebut *email* merupakan sebuah metode mengubah, mengirim, menyimpan, dan menerima pesan melalui sistem komunikasi elektronik. Istilah email meliputi sistem yang berdasar pada *Simple Mail Transfer Protocol* (STMP) dan sistem internet yang memungkinkan pengguna dalam satu organisasi mengirimkan pesan kepada satu sama lain [9].

Email terdiri dari dua bagian, yaitu *header* dan *body*. Bagian *header* membawa informasi yang dibutuhkan untuk routing e-mail, baris subjek, dan *timestamps*, sedangkan *body* terdiri dari pesan atau data yang hendak disampaikan pada penerima. Proses pengiriman email dapat dilihat pada Gambar 1. [10]

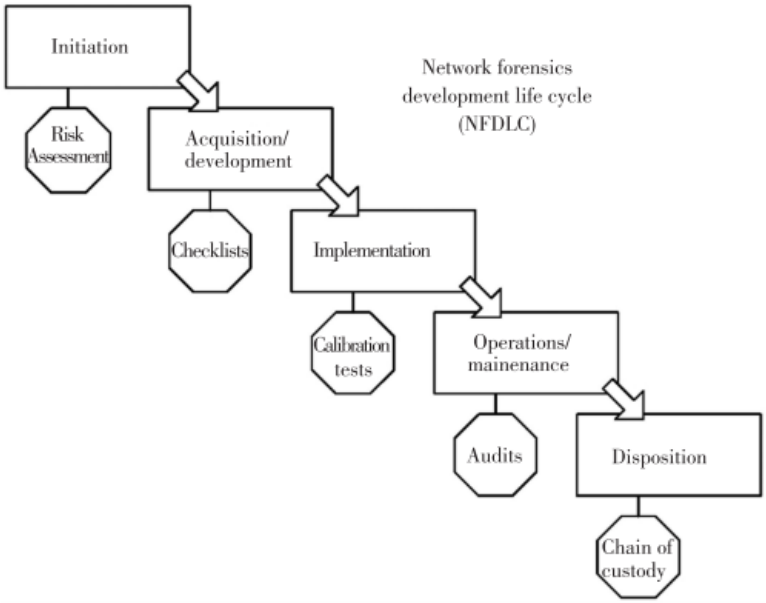


Gambar 1. Alur Proses Pengiriman E-mail

Network Forensics Development Life Cycle (NFDLC) didasarkan pada *System Development Life Cycle* (ISDLC). NFDLC telah di tunjukkan pada gambar 1. Ada lima tahapan yang harus di capai untuk memperoleh manfaat dari NFDLC. Tahapan-tahapan NFDCL antara lain inisiasi, akuisisi atau pengembangan, implementasi, operasi atau pemeliharaan, dan disposisi. Pada tahap inisiasi menentukan aspek jaringan untuk digital forensik perlindungan mengambangkan tes dasar, melakukan verifikasi, dan kalibrasi tes akan dikaitkan dengan tahap imlementasi. Operasi atau fase pemeliharaan akan menutupi pelaksanaan verifikasi dan pengukuran diambil berdasarkan audit. Pelestarian bukti dan mekanisme membuang akan tercakup dalam prosedur disposisi [11].
Spam adalah "*irrelevant or unsolicited message sent over the internet, typically to a large number of users, for the purposes of advertising, pishing, spreading malware, etc*". Dalam terjemahannya spam berarti suatu tulisan atau pesan yang tidak sesuai atau tidak berhubungan dengan topik tertentu sehingga menyebabkan ketidaknyamanan atau bahkan ketidaktepatan informasi yang diperoleh pengguna [12].
Spoofing adalah penyamaran yang menggunakan resource sistem dan fasilitas oleh pihak yang tidak bertanggung jawab. *Spoofing* adalah teknik melakukan penyamaran sehingga terdeteksi sebagai identitas yang bukan sebenarnya [13].

II. Metode Penelitian

Dalam melakukan penelitian agar mendapatkan hasil yang maksimal, tentunya harus mengikuti langkah-langkah pada metode yang telah ditetapkan. Proses penelitian ini menggunakan metode *Network Forensics Development Life Cycle* (NFDLC). Langkah-langkah metode NFDLC dapat dilihat pada gambar 2.



Gambar 2. Metode *Forensics Development Life Cycle*(NFDLC)

Gambar 1 adalah tahapan yang dilakukan berdasarkan metode yang digunakan Pemaparannya adalah :

- Initiation

  Pada tahap ini akan menentukan aspek jaringan yang akan digunakan dan dievaluasi untuk Data Forensik Perlindungan (DFP).

- Acquisition atau Akuisisi

  Akuisisi atau pengembangan berisi aturan bukti dalam sistem. Aturan bukti yang dimaksud yang berkaitan dengan kasus yang diselidiki.

- Impementation

DOI: http://dx.doi.org/10.22441/fifo.2020.v12i2.001

Implementation atau implementasi berkaitan dengan akuisisi berupa mengembangkan tes dasar, melakukan verifikasi, dan kalibrasi tes yang akan dikaitkan pada tahapan ini.

Kalibrasi adalah "penentuan akurasi instrumen,biasanya dengan pengukuran variasi dari sebuah standar" dan berguna dalam membangun bukti dasar bahwa alat yang digunakan untuk fungsi mengumpulkan bukti forensik sebagaimana dimaksud [14]

- *Operation* atau pemeliharaan

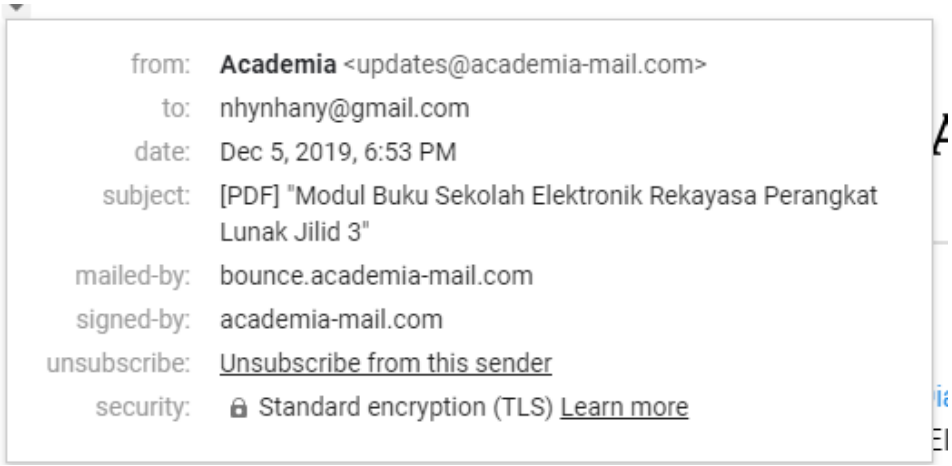
  Operasi atau fase pemeliharaan akan menutupi pelaksanaan selama verifikasi yang diambil berdasarkan audit. Dokumentasi yang akan dihasilkan akan dipelihara dan sebagai bukti bahwa jaringan dan perangkat forensik berfungsi dengan baik dan merekam sesuai dengan yang diperlukan.

- *Disposition*

  Disposition atau disposisi yang tercakup dalam pelestarian bukti dan mekanisme terhadap serangan yang dituju. Penilaian risiko, daftar periksa, kalibrasi tes, audit, dan lacak balak akan membantu lima prosedur yang disebutkan di atas kemudian setelah prosedur inisiasi.

III. Hasil Dan Pembahasan

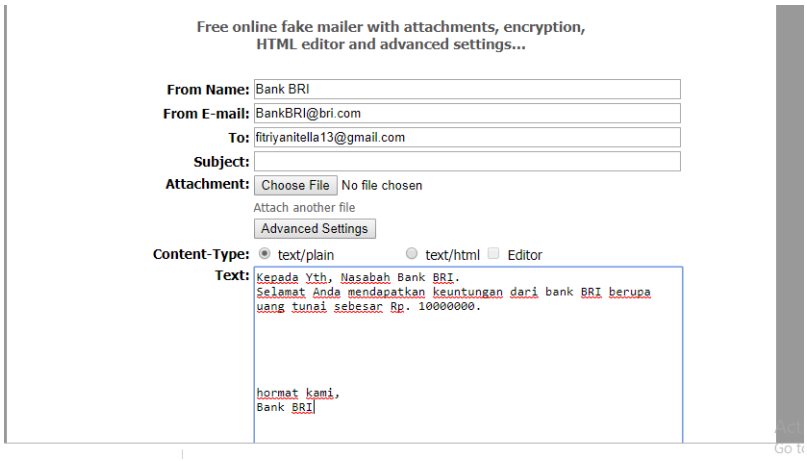
Hasil dari forensik jaringan sebuah email terhadap serangan email spoofing dan spamming berupa dapat mengetahui alamat email pengirim, alamat ip pengirim. Proses awal yang dilakukan dalam membedakan serangan email spoofing dan spamming diawali dengan forensik email membutuhkan sebuah metode seperti yang telah digunakan yaitu NFDLC. Penelitian ini dibutuhkan tools yang digunakan untuk membuat email yang digunakan untuk mendeteksi serangan spoofing. Tools yang digunakan hendaknya mempunyai hak akses bebas dan mudah digunakan. Pada serangan email spoofing akan ditemukan didalam *header* pesan seperti from, Reply-To. Dua bagian yang dijadikan yang akan dijadikan pengamayan yaitu pada *header* dan *body*. Dilihat dari sebuah *header* adalah *From* yang digunakan nama dan alamat pengirim yang mudah untuk dipalsukan, To yang digunakan adalah tujuan yang disamarkan juga dengan begitu mudah, Subject and Date akan terekam langsung dari komputer pengirim, namun jika tanggal dan jam pengirim diubah akan tidak. Jika ingin mendapatkan informasi dari pengirim lebih detail, header pada e-mail perlu diekstrak. Jika telah diekstrak, dari header tersebut akan didapatkan ip lokal dari pengirim, ID unik yang diberikan oleh server-mail, dan alamat server pengirim.
Pada tahapan yang terakhir akan dilakukan pelaporan dari hasil penelitian yang berupa barang bukti yang valid dari *e-mail* palsu tersebut, dijelaskan dalam pelaporan adalah proses dan tahapan yang akan digunakan sehingga mendapatkan barang bukti yang dibutuhkan dengan valid. Berikut adalah contoh email ditunjukkan pada Gambar 3.



Gambar 3. Header dan Body Email

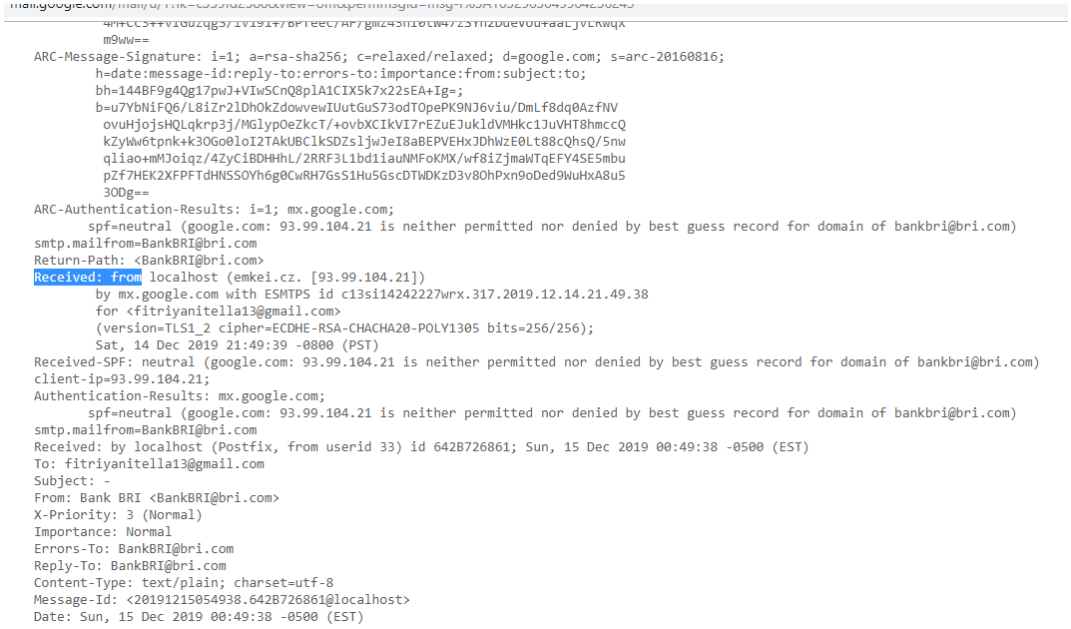
DOI: http://dx.doi.org/10.22441/fifo.2020.v12i2.001

Seperti pada simulasi diatas yang telah dijelaskan Gambar 3 merupakan salah satu cara yang dilakukan untuk mempalsukan *e-mail* pengirim. Ketika *e-mail* dikirimkan dan akan masuk ke penerima dijelaskan pada gambar 4.



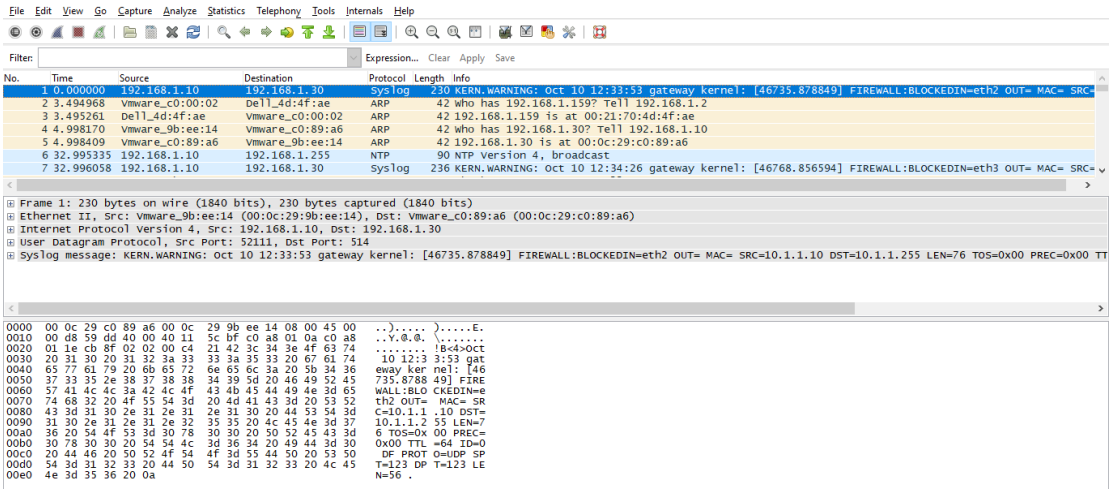
Gambar 4. Pembuatan *e-mail* palsu

Gambar 4. merupakan pembuatan *e-mail* guna untuk melakukan penyerangan *e-mail spoofing*. Selanjutnya penerima akan menerima *e-mail spoofing* tersebut, dan dilakukan penacarian *log e-mail spoofing* dan *spamming*. Pada gambar 5 akan ditampilkan *full header* pada *e-mail* pengirim. Menjelaskan banyak data yang bisa didapatkan di *full e-mail header*. Akan muncul alamat *ip address* server yang meneruskan *e-mail* dan yang kedua adalah alamat IP dari pengirim asal. IP *address* pertama adalah milik server layanan google yang diteruskan *e-mail*.



Gambar 5. *Full Header E-mail*

Mengacu pada jurnal [6] yang mengacu pada *header*. Maka pada penelitian akan ditambahkan simulasi serangan dari *attacker* ke *victim*, dan pencarian *log capture wireshark* berupa *ip address*, *source* dan *destination*, *protocol* dan *time* yang akan ditampilkan pada gambar 6.



Gambar 6. *Capture Log wireshark*

Tabel perbandingan *e-mail spamming* dan *spoofing* sebagai berikut:

Tabel 1. Perbandingan *E-mail Spamming* dan *Spoofing*

No.	*E-mail Spoofing*	*E-mail Spamming*
1.	IP Address 192.168.1.10	IP address 192.168.1.255
2.	E-mail yang dikirim dalam jumlah banyak dan terus menerus.	E-mail yang dikirim bukan dari pengguna asli
3.	ID Pesan	ID Pesan
4	Alamat Pengirim	Alamat Pengirim
5.	*Source dan Destination*	*source dan destination*

IV. Kesimpulan

Penelitian yang menggunakan metode NFDLC dengan pendekatan beberapa tools akan menghasilkan pemalsuan atau spam email berupa alamat dan tanggal *e-mail* yang palsu, mengetahui ip lokal dari pengirim, mengetahui ID pesan, dan format penyimpanan email ketika *e-mail* dipindah dan protokol yang digunakan dalam *e-mail*.

V. Daftar Pustaka

[1] Mustafa and I. Riadi, "Rancangan Investigasi Forensik E-mail dengan Metode National Institute of Justice," pp. 121–124, 2018.
[2] S. Aji, A. Fadlil, and I. Riadi, "Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 11, 2017.
[3] M. A. Sutisna, M. T. Informasi, U. A. Dahlan, I. Riadi, M. Kom, and J. Soepomo, "Analisa Forensik Pada Email Spoofing," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 38–43, 2018.
[4] L. Zhuang *et al.*, "Characterizing botnets from email spam records," *Proc. 1st Usenix Work. Large-*

Scale Exploit. Emergent Threat., no. 2, pp. 1–9, 2008.
[5] M. N. Faiz, R. Umar, and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 1, no. 3, p. 108, 2017.
[6] A. L. Suryana, R. El Akbar, and N. Widiyasono, "Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS)," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, pp. 111–117, 2016.
[7] I. Riadi and R. U. Mustafa, "Review Article : Investigasi Forensik Email dengan Berbagai Pendekatan dan Tools," vol. 04, no. 02, pp. 120–122, 2019.
[8] S. Universitas, G. Mada, and G. Mada, "Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 6, no. 2, 2013.
[9] at al Nugroho, "Aplikasi Keamanan Email Menggunakan Algoritma Rc4," *J. SAINTIKOM*, vol. 15, no. ISSN : 1978-6603, pp. 81–88, 2016.
[10] Hoiriyah, B. Sugiantoro, and Y. Prayudi, "Investigasi Forensik Pada Email Spoofing Menggunakan Metode Header Analysis," *Dasi, Amikom*, vol. 17, no. 4, pp. 20–25, 2016.
[11] D. Dhammearatchi, "Use of Network Forensic Mechanisms to Formulate Network Security," *Int. J. Manag. Inf. Technol.*, vol. 7, no. 4, pp. 21–36, 2015.
[12] A. R. C and Y. Lukito, "Deteksi Komentar Spam Bahasa Indonesia Pada Instagram Menggunakan Naive Bayes," *J. Ultim.*, vol. 9, no. 1, pp. 50–58, 2017.
[13] T. Ariyadi, "No Titleالـ جـ نائـ ية الاجـ راءات," *ABA J.*, vol. 102, no. 4, pp. 24–25, 2017.
[14] B. Endicott-Popovsky, D. A. Frincke, and C. A. Taylor, "A theoretical framework for organizational network forensic readiness," *J. Comput.*, vol. 2, no. 3, pp. 1–11, 2007.