INVESTIGATION DIGITAL FORENSIC TERHADAP SERANGAN EMAIL SPOOFING PADA PT KAI DIVRE III PALEMBANG

[1]Eggy Saputra, [2*]Misinem
[1,2]Teknik Komputer, Vokasi, Universitas Bina Darma
misinem@binadarma.ac.id

Abstract *- The Internet is an integral part of the development of modern technology and has resulted in great changes in society. Email is one that almost everyone has. Email is one of the results of developments in information and Communication Technology. Email is widely used to exchange information. Email aims to write, send, receive, and store electronic messages in the form of image, audio, video, and other files from one individual to another in various locations around the world through the internet network. Spoofing is the practice of sending an email by deliberately manipulating or spoofing the sender's address so that it looks as if the email was sent from a legitimate address., This study aims to analyze emails that are suspected to be email spoofing at PT Kai Divre III Palembang. This study uses the method of NIST (National Institute of Standards and Technology). The Email that will be used to analyze is in the header of the email using forensic tools, namely email tracer, dossier, fortiguard labs and messageheader. This analysis will check the accuracy of email headers using tools. Email that is suspected as email spoofing will be proven using tools that meet the value after analysis with various tools.*

Keywords: email Spoofing, Email headers, Live Forensics, NIST, forensic Tools

Abstrak - *Internet* adalah bagian *integral* dari perkembangan teknologi modern dan telah menghasilkan perubahan besar dalam masyarakat. *Email* menjadi salah satu yang hampir seluruh orang miliki. *Email* merupakan salah satu hasil dari perkembangan dalam teknlogi informasi dan komunikasi. *Email* banyak digunakan untuk bertukar informasi. *Email* bertujuan untuk menulis, mengirim, menerima, dan menyimpan pesan elektronik berupa berkas gambar, *audio*, *video*, dan lainnya dari satu individu ke individu lain di berbagai lokasi di seluruh dunia melalui jaringan internet. *Spoofing* adalah praktik mengirimkan email dengan sengaja memanipulasi atau memalsukan alamat pengirim sehingga terlihat seolah-olah email tersebut dikirimkan dari alamat yang sah., Penelitian ini bertujuan untuk menganalisa *email* yang diduga merupakan *email spoofing pada* PT Kai Divre III Palembang. Penelitian ini menggunakan metode *NIST (National Institute of Standards and Technology)*. *Email* yang akan digunakan untuk menganalisis yaitu pada bagian header email menggunakan *tools forensic* yaitu *email tracer*, dossier, fortiguard labs dan messageheader. Analisis ini akan memeriksa keakuratan pada header email menggukan *tools. Email* yang diduga sebagai *email spoofing* akan dilakukan pembuktian menggunakan *tools* yang memenuhi *value* setelah dilakukan analisi dengan berbagai *tools*.

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

1. Pendahuluan

Internet merupakan bagian dari perkembangan teknologi, *Internet* telah membawa banyak perubahan besar dalam masyarakat. *Email* adalah salah satu yang paling banyak digunakan di dunia. *Email* merupakan aplikasi yang sangat populer dan digunakan setiap hari untuk keperluan pribadi, bisnis atau resmi. Salah satu kejahatan paling umum adalah *spoofing email. Spoofing* adalah *email* yang dipalsukan dan dikirim seolah-olah berasal dari sumber tepercaya.

Spoofing email digunakan oleh penulis untuk menyembunyikan alamat *email* asli dengan mengubah beberapa kolom di *email*, seperti "*from*", "*return-path*", dan "*replay to*". Untuk membuat *email* terlihat seperti *email* asli dan mungkin menipu penerima yang tidak memahami *email* tersebut dan terjebak dalam skrip yang dibuat oleh penulisnya.

Setelah dilakukan pengamatan pada PT KAI divre III palembang, disini di temukan adanya indikasi ganguan, terhadap *system* pengiriman berbasis *email*. dalam melakukan *investigation* agar nantinya kendala dalam ancaman *spoofing email*, bisa dilakukan nya pencegahan dan penanganan agar dapat digunakan dengan baik. Yaitu dengan penerapan metode *NIST*(*National Institute of Standards Technology*) melakukan ananalisis terhadap bukti *digital* atau tahapan untuk mengumpulkan informasi dari bukti *digita*l.

2. Tinjauan Pustaka

2.1. Electronic E-mail(email)

Electronic E-mail atau biasa disingkat juga *email* dalam bahasa indonesia diartikan sebagai "surat elektronik" merupakan sebuah sistem yang bertujuan untuk menulis, mengirim, menerima dan menyimpan pesan *elektronik* berupa *file* gambar, *audio, video,* dan lain-lain dari satu orang ke orang lain di belahan dunia melalui jaringan *internet* [1].

2.2. Email Spoofing

Email Spoofing adalah *email* yang dikirimkan dengan sengaja di palsukans upaya terlihat seolah-olah dikirim dari *email* yang sah, sedangkan *Email Spamming* merupakan *spam* atau *junk mail* yang mengacu kepada pengiriman *email* kesembarang orang untuk tujuan yang tidak diperlukan bahkan untuk tujuan yang jahat [2].

2.3. Tools Email Dossier

Tools Email Dossier. Cara Kerja Dari *Tools* Ini Yaitu Dengan Memasukkan Ip Yang Akan Diuji. Tujuan *Email Dossier* yaitu sebagai pengecekan validitas dari *email* pengirim. Ditemukan Adanya *Ip Address* Pengirim Dan Nama *Server* [3].

2.4. Tools Email Tracer

Tools Email Treacer Cara Kerja Dari *Tools* Ini Yaitu Dengan Menganalisis *Header Email* Dan Menyediakan *Ip Address* Mesin Yang Mengirimkan *Email* Tersebut. Fungsi dari *Tools Email Treacer* yaitu *tools* ini dapat mendeteksi Daerah Dan Negara *Email* Tersebut Dikirim Diantaranya Menunjukkan *Address* Pengirim dan *ip* [4].

2.5. ToolsMessageheder

Tools Messageheder Cara Kerja Dari *Tools* Ini Yaitu Mengechek *Header Email*. Fungsi dari *Tools Messageheder* yaitu untuk Menampilkan Pengirim *Email*, Waktu Pengiriman Dan Kepada Siapa Di Kirim [5].

3. Metodologi Penelitian

3.1. Metode penelitian

metode yang akan digunakan dalam melakukan ananalisis terhadap bukti *digital* atau tahapan untuk mengumpulkan iformasi dari bukti *digital* yaitu dengan metode *NIST*(*National Institute of Standards Technology*) [6]. Langkah metode ini digunakan untuk menjabarkan proses *forensic* dalam melakukan invetgasi dan menjadi acuan dalam menaggulangi masalah pada PT KAI DRIVE III Palembang. ada beberapa metode yang akan dilakukan.

Pada tahap *collection* yaitu melakukan sebuah simuasi yang digunakan sebagai analisis. Selain dengan menggunakan *tools* yang berakaitan dengan *email spoofing*. tahap *examination* mengolah data yang terkumpul secara forensic dengan melakukan pemeriksaan menggunakan

tools. Tahap *analysis* melakukan hasil pemeriksaan menggunakan *tools*. Tahap *reporting* adalah hasil dari pemriksaan dari tindakan forensk yang dambil.

3.2. Pengumpulan (*data collection*)

Pada tahap ini dilakukan nya pengumpulan data pada PT KAI DRIVE III Palembang. Pengumpulan data adalah Identifikasi sumber yang dapat dijadikan bukti dan penjelasan langkah-langkah dalam proses pengumpulan data. Data disini adalah bukti hasil serangan *email spoofing*. Pengumpulan data mencakup beberapa fungsi, seperti berikut ini:

a. Identifikasi data, disini dilakukannya proses pembuktikan atau mengenali data, untuk tujuan agar mudah dikenali sebagai data yang telah terverifiksi sebagai objek penelitin.
b. Penandaan data, disini dilakukannya proses menandai data, dari objek penelitan agar tidak tertukar saat proses berikutnya dilakukan.
c. Penyimpanan data, disini dilakukannya proses simpan menyimpan atau merekam informasi. yang telah dilakukan pada proses sebelumya, agar pada saat melakukan tahap selanjutnya tidak ada kendala atau pun kehilangan data, yang mengakibatkan gagalnya proses dalam melakukan pengumpulan data.

3.3. *Examination* (Pengujian)

Setelah melalui prosesnya pengumpulan data, sebuah langkah maka perlu untuk menguji informasi yang diperlukan dari data yang dikumpulkan, langkah ini berarti mengabaikan atau meminimalkan properti *system* Sistem operasi dan aplikasi yang dapat mengaburkan data, seperti. Mekanisme *kompresi*, *enkripsi*, dan kontrol akses. *Hard drive* bisa berisi ribuan atau jutaan *file*, proses pemfilteran memilih beberapa data yang tidak diperlukan. Misalnya, data kinerja minggu lalu terdiri dari jutaan catatan, namun hanya ditemukan ratusan catatan yang relevan untuk ditinjau lebih lanjut.

Banyak alat dan teknik yang digunakan untuk menghilangkannya Mengerjakan Basis data, informasi berbasis teks, dan berbagai model khusus dapat digunakan untuk menentukan keakuratan informasi, seperti mencari *dokumen* yang berkaitan dengan seseorang atau subjek tertentu atau mengidentifikasi *log email* untuk menentukan *email*/dan *email.* alamat *email* yang dapat mengarah pada klarifikasi kasus ini.

Proses yang digunakan dalam pengujian ini adalah dengan menggunakan tools agar dapat mempermudah jalannya pengujan. Tools yang digunakan dalam pengujin ini antara lain yaitu :

a. *Tools Email Dossier*, Tujuan dari pengujian menggunakan *Email Dossier* yaitu sebagai pengecekan validitas dari *email* pengirim.
b. *Tools Email Treacer*, tujuan dari pengujian menggunakan *tools* ini yaitu dapat mendeteksi Daerah Dan Negara *Email* Tersebut Dikirim Diantaranya Menunjukkan *Address* Pengirim dan *ip.*
c. *Tools Fortiguard Labs*, Tujuan dari pengujian menggunakan tools ini yaitu untuk mengechek keamanan dan juga berperan sebagai *firewall* dan sekaligus sebagai pertahan utama dan pelaporan.
d. *Tools Messageheder*, Tujuan dari pengujian menggunakan tools ini yaitu, untuk Menampilkan Pengirim *Email*, Waktu Pengiriman Dan Kepada Siapa Di Kirim.

3.4. *Analysis*(Analisis)

Analisis proses dilakukan Setelah mengkaji tahapan pengujian data, analisis adalah suatu proses pengambilan keputusan yang menggunakan pendekatan metodis untuk menarik kesimpulan yang berkualitas tinggi berdasarkan ketersediaan data atau sebaliknya untuk memutuskan bahwa hasilnya tidak dapat dijadikan kesimpulan, dan ini bisa. terjadi ketika dihadapkan pada situasi nyata di lapangan.

Tahap analisis atau tahap penelitian dilakukan setelah memperoleh *file* atau *data digital* yang diinginkan pada pemeriksaan sebelumnya menggunakan *tools*. Data dari adanya *email spoofing*, tersebut kemudian dianalisis secara rinci dengan menggunakan metode yang

digunakan, untuk dapat membuktikan data *email spoofng*. Hasil analisis data *email spoofing* kemudian dijadikan bang bukti digital dan dapat diinterpretasikan secara ilmiah dan hukum.

3.5. *Reporting* (dokumentasi dan laporan)

Pelaporan adalah langkah terakhir dalam proses forensik komputer. Pada langkah ini kami menyajikan data yang merupakan hasil proses analisis. Banyak faktor yang dapat memengaruhi pelaporan.Pada tahap pelaporan atau tahap *Reporting* setelah dilakukanya poses pengechekan dan analisis barang bukti data dari tools. Selanjutnya, pada tahap ini juga dilakukan pelaporan hasil analisis uraian tindakan yang akan dilakukan, penjelasan alat, dan metode yang digunakan, mengidentifikasi tindakan pendukung yang harus diambil, dan membuat rekomendasi untuk memperbaiki kebijakan, metode, tools, atau aspek pendukung lainnya dari sejumlah proses tindakan forensic [7].

Dalam penelitian ini, bukti digital yang digunakan bukan diperoleh dari lingkungan nyata atau bukti *digital* tersebut tidak diperoleh dari hasil kejahatan komputer yang sebenarnya namun bukti digital dalam penelitian ini dihasilkan dan diperoleh dari hasil simulasi yang dilakukan pada *email* Pt Kai Drive III Palembang. Penerapan dan pengujian dilakukan dengan menggunakan Skenario tersebut bertujuan untuk mendapatkan bukti digital seperti pada kasus kejahatan komputer nyata [8].

Langkah-langkah untuk mengidentifikasi *tools forensik* yang tepat menemukan bukti kejahatan dunia maya dalam penelitian ni adalah berikut ini:

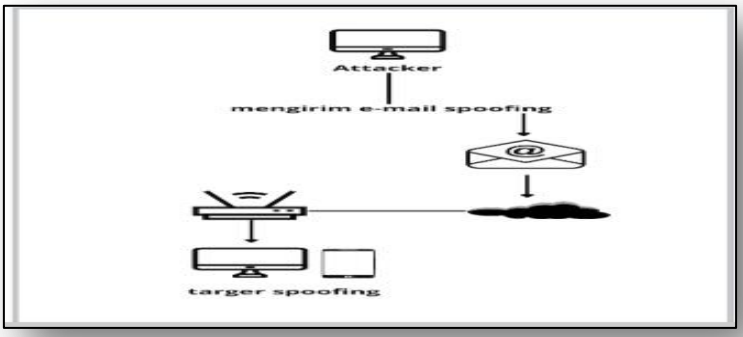
1. *tools* yang digunakan harus sesuai dengan spesifikasi *device* penguji.
2. *tools* yang digunakan dapat menampilkan informasi lengkap tentang waktu terjadi, alamat pengim dan infomasi penunjang lain nya.
3. *tools* ini tidak berbayar atau gratis

Langkah-langkah untuk menentukan aspek hukum yang berlaku dari kasus-kasus yang disimulasikan, yaitu peneliti mempelajari dan mendalami UU ITE dan KUHP, lalu menghubungkannya Hukum dengan kasus simulasi dalam penelitian ini [9]. Peneliti melakukan uji tuntas hukum dengan ahli hukum untuk memastikannya bahwa hukum yang diterapkan cocok untuk kasus yang disimulasikan [10].

4. Hasil dan Pembahasan

4.1 *Pembahasan Alur Email Spoofing*

Investigasi barang bukti dalam penelitian menggunakan *tools forensic* yaitu *email tracer, dossier, fortiguard labs* dan *messageheader*. Proses pengambilan *email* dilakukan dengan simulasi sebagai serangan untuk melakukn *email spoofing*, yang akan ditunjukan pada gambar 1.

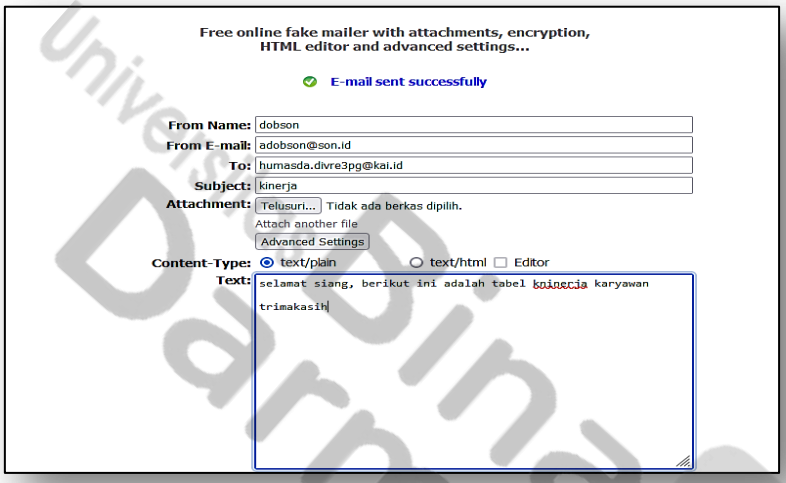


Gambar 1**.** Alur simulasi *Emil Spoofing*

P-ISSN 2654-5438
E-ISSN 2828-4917

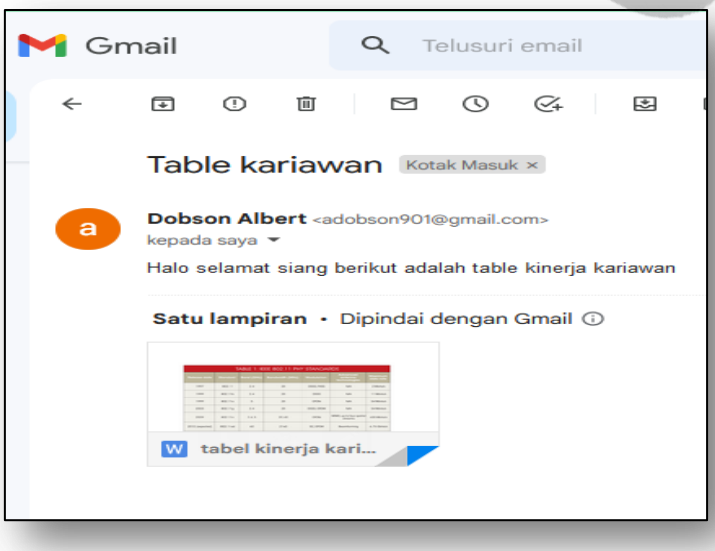
Pada gambar 1. merupkan alur simulasi dari *email spoofing*. Hal pertama yang akan dilakukan adalah membuat *email* palsu dan mengirimkan kepada korban seolah-olah *email* yang dikirim berasal dari pemilik *email* yang asli. Setelah *email* diterima oleh korban, kemudian dari bukti *email* tersebut akan dilakukan analisis menggunakan beberapa *tools* tersebut.

Proses pengiriman *email* menggunakan *tools Emkei'z fake emails*. Pengirim *email* korban adalah humasda.divrepg@kai.id dan e*mail* pelaku yaitu adobson901@gmail.com. *Email* yang telah terkirim berisikan table kinerja karyawan , dapat dilihat pada gamabar 2.



Gambar 2. Pengiriman *Email Spoofing*

Pada proses pengiriman *email* yang pertama dialakukan dengan mengirimkan *email* menggunakan *email* yang asli yaitu menggunakan situs resmi *gmail.com*, berikutnya menggunakan *tools Emkei'z fake emails* untuk pengiriman *email spoofing*. Sedangkan pada gambar 3 dan 4 merupakan isi *filed email* yang di terima oleh pelaku terhadap korban.



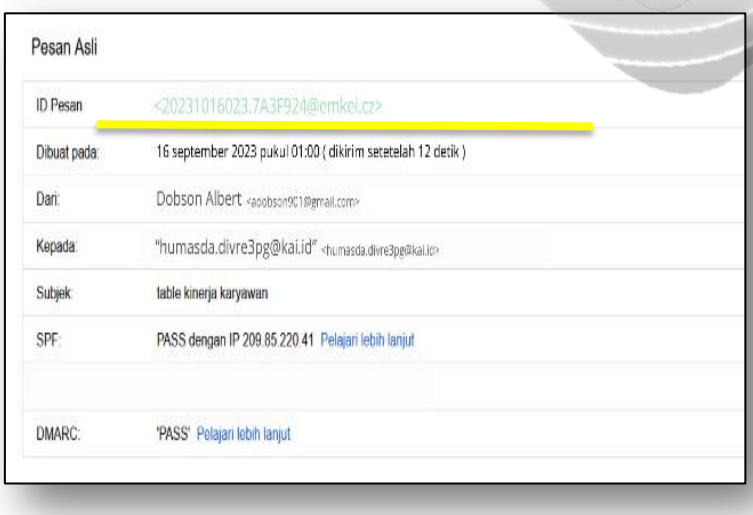
Gambar 3. *Field Email Yang Valid*

P-ISSN 2654-5438
E-ISSN 2828-4917

Pada gambar 3 adalah *Field Email Yang Valid,* yang dikirim melalui situs resmi *gmail.co*. sedangkan pada gambar 4 adalah *Field Email Spoofing* yang di kirim melalui *tools Emkei'z fake emails.*

Gambar 4. *Field Email Spoofing*

Jika kita perhatikan pada gambar 3 dan Gambar 4 sedikit tidak ada perbedaan isi *field* antara kedua *email* tersebut. Isi *field* kedua *email* tersebut terlihat serupa. Tapi jika dianalisis kembali, *email* tersebut terdapat perbedaan yang datang dari pengirim yang mengirimkan email atau alamat *email* yang berbeda atau tempat yang tidak sama. Bukti yang dapat dilihat di *header* kedua *email* tersebut.



Gambar 5. *Header Email Spoofing*

P-ISSN 2654-5438
E-ISSN 2828-4917

Gambar 6. *Header Email* Asli

Terlihat Pada Gambar 5 *email spoofing* yang dikirimkan pelaku pada ID pesan spoofing tersebut merupakan *email emkei'z fake* bukan dari *gmail*. sedangkan pada Gambar 6, email tersebut merupakan *email* asli yang dikirim langsung melalaui situs *Gmail*. Maka dapat di idendifikasikan *email* yang di terima adalah *email spoofing*.

4.2 Hasil Analisis *Tools Dossier*

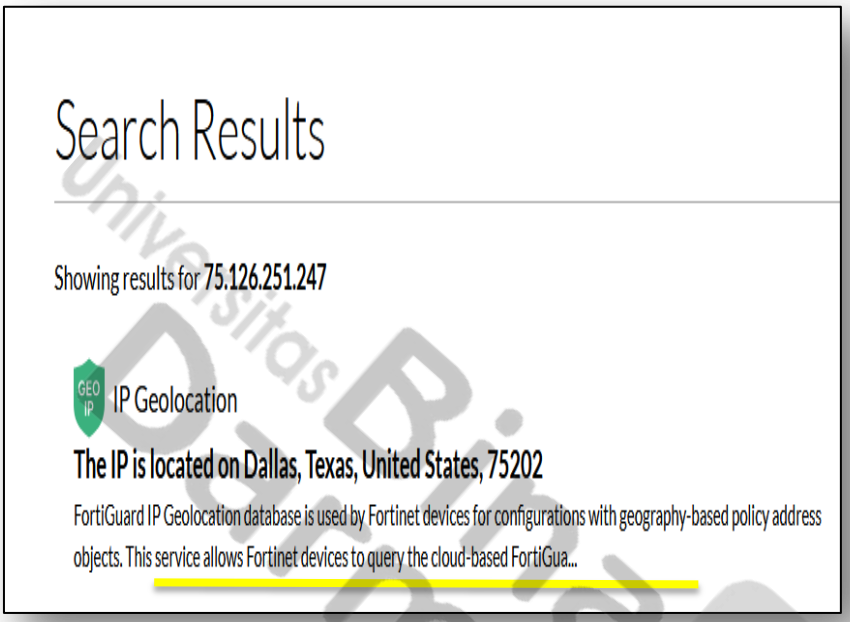
Berikutnya akan dilakukan pengujian *email spoofing*. Analisis pertama yang akan dilakukan menggunkan *tools dossier* seperti pada Gambar 7

.

Gambar 7. Hasil Menggunakan *Email Doossier*

P-ISSN 2654-5438
E-ISSN 2828-4917

Pada Gambar 7. pengujian menggunakan *email dossier*. Cara kerja dari *tools* ini yaitu dengan memasukan nama *email* atau *ip* yang akan diujikan. Penguji akan menggunkana *email dossier* ditemukan nama dan *ip address* pengirim dan *server*. Menunjukan *address* pengirim, *email* pengirim dan admin. Disini *tools Email Doossier* bertujuan untuk pengechekan validasi dari alamat pengirm *email*, apakah benar alamat dari pengirm tesebut benar-benar *valid*.

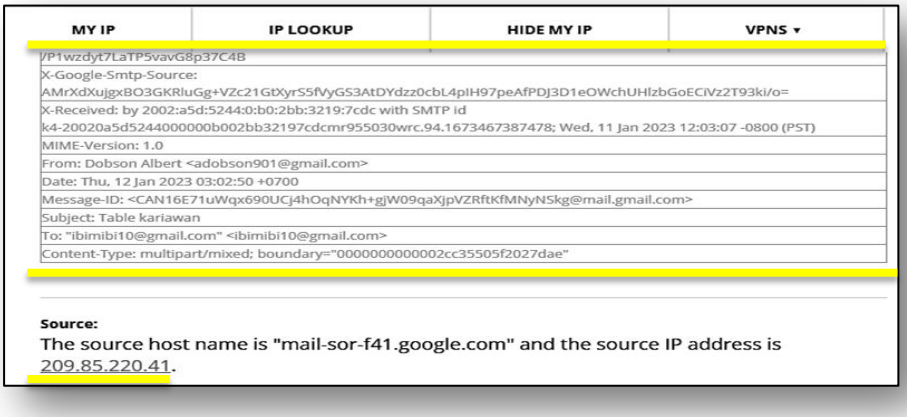


Gambar 8. Hasil Menggunakan *Fortiguard Labs*

4.3 Hasil Analisis Menggunakan *Tools Fortiguard Labs*

Selanjutnya dianalisis kedua menggunakan *tools fortiguard labs*. cara kerja dari *tools* ini dengan memasukan *ip address* dan akan di periksa. *fortiguard labs* akan meneliti ancaman apa saja dan aktifitas apa saja yang terjadi, contoh seranga *cyber*. lalu *fortiguard labs* akan menganalisis dan memproses informasi ini menggunakan *AI*.

Dapat dilihat di gambar 8 dari pengechekan menggnakan *tools fortiguard labs*, dapat dilihat lokasi dari pengirim baik dari kota, maupun Negara asal dari pengirim yang tedeteksi oleh *system* pada *tools fortiguard labs.*



Gambar 9. Hasil menggunakan *tracer Email*

4.4 Hasil Pengujian Menggunakan *Mesageheader*

Pengujian menggunakan *Mesageheader*. Pada pengujian cara kerja dari *Mesageheader* yaitu menyediakan daftar detail teknis tentang pesan, seperti siapa pengirim yang mengirimnya dan perangkat lunak yang digunakan untuk membuatnya, *server email* yang dilaluinya ke pengirim dan *messageheader* sama dengan beberapa *tools* lain nya, cara mengaksesnya yaitu dengan cara memasukan *header* dari *email*, dapat dilihat pada gambar 10. dan dapat dilihat pada gambar di atas hasil dari pengechekan yang dilakukan menggunakan *tools Mesageheader.*

Table 1. Hasil Indikasi *Tools*

Indikasi	Email Dosseir	Fortiguard Labs	Tracer Email	Mesageheader
Server Email	√	√	√	√
Received From	-	-	√	√
Received From User	-	-	√	√
Source Ip Add	√	√	√	√
Host Name	√	-	√	√
Data Sent	√	√	√	√

Berdasarkan *table* 1. yang menjelaskan hasil dari *email spoofing* berdasarkan *tools forensics* yang telah digunakan yaitu *Email Dosseir, Fortiguard Labs, Tracer Email, Mesageheader*. Dari ke empat *tools* tersebut menjelaskan proses dan analisis pada *email spoofing* dapat dibuktikan dari mana *email* tersebut dikirim, *IP address*, alamat, *domain email*. Sehingga bisa dikatakan bahwa *email* yang dianalisi benar-benar merupakan *emai spoofing*.

Table diatas menjelaskan tentang keunggulan pada setiap *tools*, yang digunakan contoh jika di tandai dengan contreng, maka tools tersebut dapat menampilkan apa yang tertera pada bagian table, yang sudah dilakukan pengechekan.

5. Kesimpulan

1) Berdasarkan hasil pengujian *email* dan analisis yang telah dilakukan untuk mengetahui ciri-ciri dari *email spoofing*. *Email* yang ingin dipalsukan adalah pada bagian *header email*.
2) Penelitian ini menggunakan *metode live forensic* dan *NIST*, dimana *computer* tetap dalam keadaan aktif.
3) Analisis yang telah dilakukan adalah pada bagian *header email* yang rincih pada alamt *email* yang di terima. *Tools* yang digunakan adalah *Email Dosseir, Fortiguard Labs, Tracer Email*, *Mesageheader*. *Tools* yang digunakan menghasilkan barang bukti *email spoofing* yang telah melewati pengujian dengan *value tools* yang sangat baik.
4) Dari hasil penelitian ini, dapat dijadikan barang bukti, sehingga perlu dilakukan analisis lebih jauh lagi agar mendapatkan hasil barang bukti *forensic* yang lebih *relavan*.

Referensi

[1] I. Riadi, Sunardi, and F. T. Nani, "Analisis Forensik pada Email Menggunakan Metode National Institute of Standards Technology," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 2, pp. 83–90, 2022, doi: 10.14421/jiska.2022.7.2.83-90.

[2] I. Riadi, S. Sunardi, and F. T. Fitri, "Spamming Forensic Analysis Using Network Forensics Development Life Cycle Method," *INTENSIF J. Ilm. Penelit. dan Penerapan Teknol. Sist. Inf.*, vol. 6, no. 1, pp. 108–117, 2022, doi: 10.29407/intensif.v6i1.16830.

[3] A. Bachtiar, P. Studi, S. Komputer, F. Teknologi, I. Universitas, and S. Raya,

"ANALISIS WEB PHISHING MENGGUNAKAN METODE NETWORK FORENSIC DAN BLOCK ACCESS SITUS DENGAN," vol. 10, no. 1, pp. 71–83, 2023.

[4] E. Altulaihan, A. Alismail, M. M. Hafizur Rahman, and A. A. Ibrahim, "Email Security Issues, Tools, and Techniques Used in Investigation," *Sustain.*, vol. 15, no. 13, pp. 2–28, 2023, doi: 10.3390/su151310612.

[5] Y. P. Prawira and S. Samsudin, "Live Forensics Analysis Of Malware Identified Email Crimes To Increase Evidence Of Cyber Crime," *Digit. Zo. J. Teknol. ...*, vol. 13, no. 2, pp. 111–124, 2022, [Online]. Available: http://journal.unilak.ac.id/index.php/dz/article/view/11570%0Ahttp://journal.unilak.ac.id/index.php/dz/article/download/11570/4475

[6] M. Mushlihudin and A. Nofiyan, "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology," *Cybernetics*, vol. 4, no. 02, pp. 11–23, 2021, doi: 10.29406/cbn.v4i02.2287.

[7] U. B. Darma, P. M. Kanievpe, T. D. Purwanto, F. Vokasi, and U. B. Darma, "ANALISA KUALITAS JARINGAN INTERNET 4G LTE PROVIDER TELKOMSEL , IM3 DAN 3 DI KOTA PRABUMULIH," pp. 83–96.

[8] T. Amelia and D. Komalasari, "Analisis Sistem dan Prosedur Pemberian Kur Mikro pada Aplikasi Brispot BRI Unit Sudirman Palembang," pp. 33–40, 2023, [Online]. Available: https://ejournal.bsi.ac.id/ejurnal/index.php/perspektif/article/view/2495/2057

[9] Y. E. Suzuki and S. A. S. Monroy, "Prevention and mitigation measures against phishing emails: a sequential schema model," *Secur. J.*, vol. 35, no. 4, pp. 1162–1182, 2022, doi: 10.1057/s41284-021-00318-x.

[10] K. Shen *et al.*, "Weak links in authentication chains: A large-scale analysis of email sender spoofing attacks," *Proc. 30th USENIX Secur. Symp.*, pp. 3201–3218, 2021.

.