JIMP - Jurnal Informatika Merdeka Pasuruan
Vol 5 No 3 Desember 2020
ISSN 2503-1945

Validasi E-Mail Spoofing

Mochammad Arief Sutisna[1], Abdul Fadlil[2], Imam Riadi[3]
[1,2,3]Jl. Dr. Soepomo Sh no.80, Waroengboto, Umbulharjo,Yogyakarta, Indonesia.
Magister Teknologi Informasi,Universitas Ahmad Dahlan
E-mail : **m_arief_sutisna@stmikmj.ac.id[1]**, fadil@mti.uad.ac.id[2], imam.riadi@mti.uad.ac.id[3]

Abstract

E-mail is software that provides facilities for sending digital based letters and makes it easy to communicate and exchange information. So that it is possible to misuse e-mail to obtain information illegally by changing the identity of the e-mail sender and identities such as e-mail originating from legitimate e-mails (valid e-mails), this activity is commonly known as e-mail spoofing. To view e-mail spoofing requires e-mail forensic against e-mail spoofing. One of the e-mail forensic interest techniques is using e-mail header analysis (header analysis method). This technique works by checkingand comparing the values contained in several email headers that are specified as email spoofing detection parameters. The parameters used in this study are the header 'From', 'Message-ID', 'Date' and 'Received'. If the values contained in the header are identical, then the email is a valid email (valid email), otherwise the email is categorized as a spoofing email.

Keywords: *E-mail forensics, Legitimate e-mail, E-mail spoofing, Header Analysis*

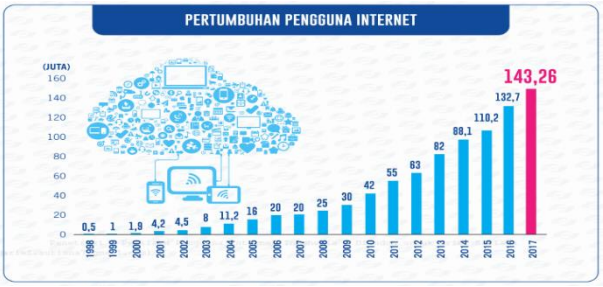
Abstraks

E-mail merupakan merupakan software yang memberikan fasilitas untuk mengirimkan surat berbasis digital dan memudahkan untuk komunikasi dan bertukar informasi. Sehingga memungkinkan menyalahgunakan e-mail untuk mendapatkan informasi secara ilegal dengan mengubah identitas pengirim e-mail dan menjadikannya seperti e-mail yang berasal dari e-mail yang sah (legitimate e-mail), aktivitas tersebut biasa dikenal dengan istilah e-mail spoofing. Untuk mengetahui e-mail spoofing diperlukan forensik e-mail terhadap e-mail spoofing. Salah satu teknik investigasi forensik e-mail adalah menggunakan analisis header e-mail (header analysis method). Teknik ini bekerja dengan memeriksa dan membandingkan value yang terdapat pada beberapa header e-mail yang ditetapkan sebagai parameter deteksi e-mail spoofing. Parameter yang digunakan dalam penelitian ini adalah header 'From','Message-ID', 'Date' dan 'Received'. Jika value yang terdapat pada header tersebut identik, maka e-mail tersebut adalah e-mail yang sah (legitimate e-mail), jika tidak maka e-mail tersebut dikategorikan sebagai e-mail spoofing.

Kata Kunci : *Forensik e-mail, Legitimate e-mail, E-mail spoofing, Header Analysis*

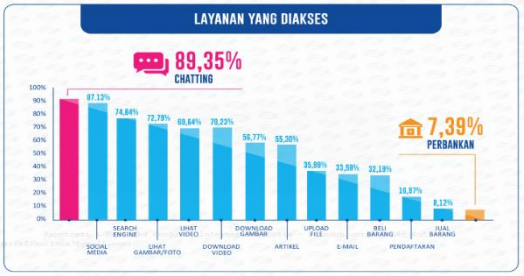
I. Pendahuluan

Internet sangat berperan dalam membantu manusia untuk melakukan segala aktivitasnya tanpa terikat oleh tempat dan waktu. Kemudahan dan tidak terbatasnya jangkauan internet, membuat pertumbuhan internet kian meningkat tiap harinya, pertumbuhan internet secara global mengalami peningkatan sebesar 143 juta di tahun 2017. (Kompas.com dikutip dari data APJII).[1]



Gambar 1. Presentase pengguna Internet di Indonesia tahun 2018 (APJII)

Fasilitas internet yang disediakan dan yang paling banyak digunakan adalah e-mail. E-mail adalah singkatan dari surat elektronik (*electronic-mail*). Dari arti tersebut sudah dapat dipahami bahwa e-mail merupakan surat elektronik yang penggunaannya menggunakan internet. E-mail terus berkembang dengan fitur-fitur yang dapat mengirim e-mail tidak hanya berbetuk teks tapi juga dapat dalam bentuk file audio, video, photo dan file ektensi lainnya.



Gambar 2. Presentase pengguna e-mail di Indonesia tahun 2018 (APJII)

Tetapi dalam kemudahan penggunaan e-mail ada ancaman serius yang dibawa oleh e-mail ke korban, karena dengan memanfaatkan e-mail sebagai media untuk melakukan perbuatan yang merugikan di dunia siber, karena e-mail merupakan alat transportasi utama bagi *spam* dan konten berbahaya dalam jaringan. E-mail bisa menjadi sumber utama dari kebanyakan aktivitas kriminal pada internet. Salah satu ancaman dari tindak kejahatan yang menggunakan e-mail adalah *e-mail spoofing* atau lebih dikenal pemalsuan atau penipuan menggunakan e-mail.

II. Tinjauan Pustaka

Teknik yang digunakan dalam penelitian *e-mail spoofing* dengan menggunakan teknik *header analysis* telah banyak dilakukan, seperti penelitian yang dilakukan oleh Wahyudi (2008). Penelitian dilakukan terhadap *e-mail spoofing* dengan menganalisis *header e-mail* yang berfokus pada objek alamat e-mail (*e-mail address*), komponen yang dianalisis adalah *Return-path* dan *Message ID* dengan metode mencocokkan *value* yang tersimpan pada kedua komponen tersebut. Penelitian serupa juga dilakukan oleh Ghawate, Patel, Bargaje, Kadam, & Khanuja (2015) dengan memanfaatkan komponen *return-path* dan *from,* penelitian tersebut berfokus pada alamat e-mail. [2] Analisis *header e-mail spoofing* juga merupakan teknik yang dapat dilakukan dengan menganalisis alamat pengirim e-mail. selanjutnya Jayan & S (2015) serta mengusulkan teknik analisis *header e-mail* terhadap *time and date* yang difokuskan pada komponen *received*[3]. Penelitian tersebut berfokus pada tanggal pengiriman dan penerimaan e-mail. Mishra, Pilli, & Joshi (2012) yang melakukan penelitian terhadap *e-mail spoofing* dengan membandingan waktu pengiriman e-mail *(sending time)* dan waktu penerimaan pesan *(last server e-mail receiving time).*[4]

Mengacu pada referensi dari penelitian terdahulu, maka penelitian ini bertujuan untuk mengetahui bagaimana mengidentifkasi status keabsahan sebuah e-mail berdasarkan tanggal dan alamat sebuah e-mail sebagai wujud kombinasi dari hasil peneliti yang pernah dilakukan oleh peneliti lain. Teknik memutuskan tersangka / terdakwa bersalah dan/atau tidak bersalah.

Validasi

Validasi diartikan sebagai suatu **tindakan pembuktian** dengan cara yang sesuai bahwa tiap bahan, proses, prosedur, kegiatan, sistem, perlengkapan atau mekanisme yang digunakan dalam produksi dan pengawasan akan senantiasa mencapai hasil yang diinginkan.

Definisi Validasi adalah konfirmasi melalui pengujian dan penyediaan bukti objektif bahwa persyaratan tertentu untuk suatu maksud khusus dipenuhi.(standar ISO/IEC 17025:2005). Validasi pada umumnya digunakan untuk metode yang tidak baku, metode yang di kembangkan atau metode yang telah dimodifikasi. Validasi biasa dilakukan untuk memastikan bahwa metode pengujian maupun kalibrasi yang dilaksanakan harus sesuai dengan penggunaan yang dimaksudkan, dan mampu untuk menghasilkan data yang valid.

Digital Forensic

Computer/digital forensic merupakan sebuah aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (pro justice), yang dalam hal ini untuk membuktikan kejahatan berteknologi tinggi atau computer crime secara ilmiah (scientific) hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut (Al-Azhar, 2012)[5]

Menurut Karie & Venter (2014) disiplin ilmu digital forensics memiliki beberapa cabang utama dan setiap cabang memiliki sub-sub tersendiri, salah satu dari cabang tersebut adalah network forensics yang didalamnya terdapat kategori internet forensics.[6]

Komputer Forensik

Komputer Forensik menurut beberapa ahli diantaranya :

- Nugroho Budhisantoso, kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisis data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum
- Judd Robin, komputer forensik merupakan penerapan sederhana dari penyidikan komputer dan teknik analisisnya dalam menentukan berbagai bukti hukum yang memungkinkan
- Ruby Alamsyah, komputer forensik atau digital forensik ialah suatu ilmu yang menganalisis barang bukti secara digital hingga dapat dipertanggungjawabkan di pengadilan, yang termasuk barang bukti digital tersebut antara lain seperti laptop, handphone, notebook, dan alat teknologi lain yang memiliki tempat penyimpanan dan dapat dilakukan analisis

Internet forensics adalah suatu usaha tentang bagaimana kita menelusuri dan menginvestigasi sumber-sumber kejahatan internet dan sekaligus mempelajari bagaimana hal itu bisa terjadi (Rafiudin, 2009)[7].

E-mail

E-mail merupakan surat elektronik yang memungkinkan semua orang dapat saling berkirim pesan dengan jaringan internet (Ali Zaki dan Smitdev Community).

E-mail merupakan salah satu fasilitas di internet yang sangat populer dan merupakan fasilitas yang paling awal dikembangkan di internet. Dengan menggunakan e-mail, kita dapat menyusun, mengirimkan, membaca, membalas, dan mengelola pesan secara elektronis dengan mudah, cepat, tepat, dan aman (Erima Oneta dan Yosep. S)[8].

Sebuah *email* memiliki tiga bagian dasar. Petama adalah **Header**, yaitu satu set baris yang mengandung informasi tentang transmisi pesan, seperti alamat pengirim, alamat penerima, atau cap yang menunjukkan waktu ketika pesan dikirim oleh server perantara untuk agen transportasi (MTA), yang bertindak sebagai kantor pemilah surat elektronik (*Jean-François Pillou)[9]*.

Pasupatheeswaran (2008) menyatakan bahwa e-mail 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.

Investigasi yang akan digunakan dalam penelitian ini adalah teknik *header analysis* dengan menggunakan *field 'From', 'Message-ID', 'Date'*, dan '*Received*' sebagai parameter deteksi *e-mail spoofing*.

E-mail spoofing

Sistem kerja Email spoofing adalah memalsukan header email agar terlihat email tersebut dikirim oleh orang lain, bukan alamat email dari pengirim aslinya. Hal ini sering terjadi guna mengelabuhi penerima dalam menyampaikan pesan berbahaya, seperti SPAM ataupun password penting

E-mail spoofing adalah Pengiriman e-mail yang tidak menggunakan identitas asli. *Spoofing* adalah sebuah teknik yang biasa digunakan oleh *spammer* dan *scammer* untuk menyembunyikan alamat e-mail asli dengan mengubah beberapa field yang terdapat pada e-mail, seperti "*From", "Return-Path", dan "Replay To", field* itulah yang dimanfaatkan oleh *spammer/scammer* untuk membuat e-mail yang nampak seperti dari pengirim yang sebenarnya dan mengelabui penerima sehingga penerima e-mail yang kurang hati-hati dan tidak memahami terhadap e-mail yang masuk akan terjebak dalam skenario yang sudah di design oleh *scammer* . Banday (2011)[10].

Header E-mail

Header merupakan catatan lengkap perjalanan sebuah e-mail sebelum sampai ke alamat e-mail yang dituju (Chandraleka, 2009)[11]. *Header* terdiri dari beberapa *field* seperti :

1. *'From'* berisi alamat e-mail pengirim.
2. *'Subject',* berisi informasi tentang topik dari ebuah pesan e-mail.
3. *'To',* berisi alamat tujuan pengiriman e-mail.

4. *'Date',* berisi tanggal pengiriman e-mail.
5. *'Cc',* atau *Carbon copy* berisi alamat e-mail yang lain selain alamat e-mail utama.
6. *'Bcc',* atau *Blind carbon copy* sama halnya dengan '*Cc*', badanya adalah penerima e-mail tidak dapat melihat alamat e-mail lain yang terdapat pada kolom '*Bcc*'.
7. *'Received',* berisi informasi tentang mail server yang dilewati oleh e-mail selama proses transmisi.
8. *'Return-Path',* berisi alamat e-mail yang berfungsi sebagai mailbox untuk menarik kembali e-mail yang dikirim jika e-mail tersebut gagal terkirim.
9. *'Message-ID',* merupakan nomor yang *unique* sebagai identifikasi e-mail.
10. *'Reply-To'*, berisi alamat e-mail jika penerima e-mail ingin membalas sebuah e-mail yang diterimanya.

Header Analysis

Header analysis merupakan analisis yang dilakukan pada metadata *header* e-mail, dimana metadata tersebut mengandung informasi tentang pengirim dan/atau jalur yang dilalui oleh pesan selama dalam perjalanan menuju alamat e-mail yang dituju, Banday (2011)[12].

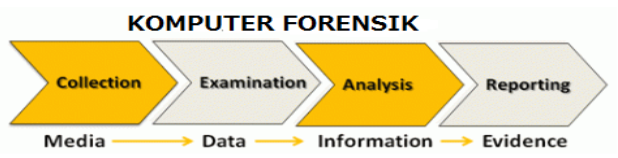
III. Metodologi Penelitian

Metodologi dalam penelitian ini menggunakan metodologi *Live Forensics* dan terdapat beberapa tahapan diantaranya yaitu :

a. Pengumpulan (*Collection*),
b. Pengujian (*Examination*),
c. Analisa (*Analysis*),
d. Laporan (*Reporting*).

Seperti yang dijelaskan dalam Gambar 4. tentang alur metodologi *Live Forensics*.

Gambar 4 Tahap-tahap komputer *forensics*



Pada Gambar 4 diatas menjelaskan tahapan dari proses investigasi digital forensik dari NIST. tahapan dari metode diatas yaitu *: Collection, Examination, Analysis,* dan *Reporting* (Kent, Chevalier, Grance, & Dang, 2006)

1. *Collection* (Pengumpulan Data)

Pengumpulan data adalah mengidentifikasi sumber-sumber yang dianggap dapat untuk dijadikan barang bukti, dan menjelaskan langkah-langkah yang dibutuhkan dalam proses pengumpulan data. Pengumpulan data melingkupi beberapa aktifitas seperti berikut :

1. Identifikasi
2. Penamaan (*Labeling*)
3. Perekaman (*Recording*)
4. Mendapatkan data

2. *Examination* (Pengujian)

Setelah melalui proses pengumpulan data, langkah selanjutnya yaitu dengan melakukan pengujian terhadap data yang relevan dari data-data yang telah dikumpulkan, tahapan ini melibatkan *bypassing* atau meminimalisasi fitur-fitur sistem operasi dan sistem aplikasi yang dapat mengaburkan data, seperti *kompresi, enkripsi* dan akses mekanisme kontrol.

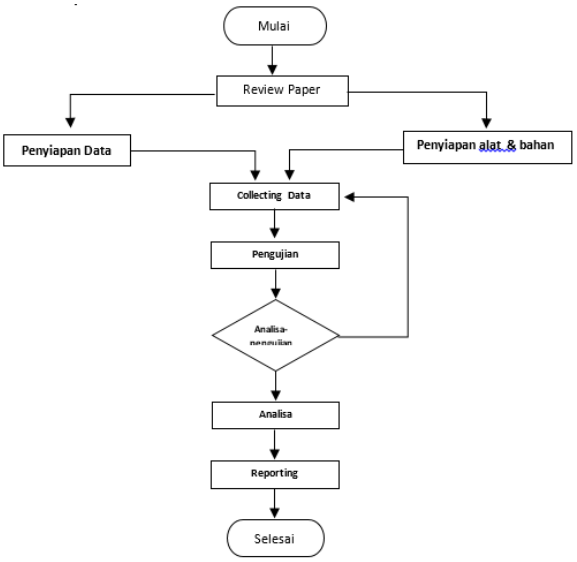
Hard drive dapat berisi ribuan atau jutaan *file*, proses *filtrasi* akan menyeleksi sebagian data yang tidak dibutuhkan, contoh data *log* kegiatan minggu lalu yang terdiri dari jutaan *record* akan tetapi didapati hanya ratusan *record* saja yang dinilai penting untuk proses pemeriksaan lebih lanjut. Ada banyak peralatan dan teknik yang digunakan untuk melakukan eliminasi terhadap tumpukan data, pencarian data berbasis teks dan berbagai pola tertentu dapat digunakan untuk mengidentifikasi ketepatan suatu data, seperti pencarian terhadap dokumen yang berhubungan dengan seseorang atau pokok permasalahan tertentu, atau mengidentifikasi pada *e-mail log entries* untuk mendapatkan email/dan alamat email yang dapat mengarahkan kepada pencerahan kasus.

3. *Analysis* (Analisis)

Proses *analysis* dilakukan setelah melalui tahapan *pengujian* informasi, Analisa adalah proses pengambilan keputusan dengan menggunakan pendekatan metodis untuk dapat menghasilkan kesimpulan yang berkualitas berdasarkan pada ketersediaan data atau sebaliknya, dengan menyimpulkan bahwa tidak memperoleh hasil yang dapat dijadikan kesimpulan, dan itu dapat terjadi ketika menghadapi situasi real di lapangan tidak memungkinkan.

4. *Reporting* (Dokumentasi dan Laporan)

Reporting adalah tahapan akhir dari proses *computer forensics*, dalam tahapan ini kita akan merepresentasikan informasi yang merupakan hasil dari proses analisis, banyak factor yang dapat mempengaruhi reporting seperti yang akan dibahas berikut ini :



Gambar 5. *Flowchart* Tahapan *Forensics* Metode NIST

Alat dan Bahan

Alat dan bahan yang digunakan untuk membantu dan menyelesaikan penelitian ini terdiri dari *hardware* dan *software*. Table 1 adalah beberapa alat dan bahan yang digunakan dalam penelitian ini.

Tabel 1. Alat dan Bahan Penelitian

No.	Nama Alat dan Bahan	Deskrifsi / Spesifikasi	Keterangan
1.	Komputer/Laptop	Core i3 Ram 4 GB HDD 250 GB	Hardware
2.	Modem	Alat untuk melakukan Koneksi internet	Hardware
3.	Internet	Proses koneksi internet lewat ISP	Jasa Internet
4.	*MailXaminer*	Melakukan pencitraan drive dan melestarikannya dalam format E01.	Software
5.	*Iptrackeronline*	alat investigasi email canggih yang mendukung lebih dari 20 format email dan sekitar 750 format MIME.	Software
6.	*Ip-adress tracer*	Dapat melihat gambar lokasi sipengirim email palsu	
7.	*Email Doisser*	Untuk mendeteksi address email dengan mengcopy email address	Software
8.	*Ipnetinfo*	Alat investigasi menyeluruh dikenal untuk penyelidikan forensik dari email	Software
9.	*DNSSetuff*	melalui dekripsi dalam email.	Software

E-mail Forensics

E-mail forensics mengacu pada studi tentang sumber dan isi e-mail sebagai alat bukti untuk mengidentifikasi pengirim e-mail yang sebenarnya dan penerima e-mail, tanggal / waktu ketika e-mail ditransmisikan, *detail record* tentang transaksi e-mail Banday (2011)[10]. untuk dapat melakukan *e-mail forensics* terdapat beberapa teknik investigasi dalam melaksanakannya, sedangkan menurut Karsono (2012) forensik e-mail adalah suatu tindakan pengamanan, pengecekkan, serta penelusuran terhadap e-mail palsu. Metode yang digunakan dalam penelitian ini adalah metode observasi, yaitu metode pengumpulan data yang akan diamati secara langsung. Objek pengamatan dalam penelitian ini adalah *header e-mail*. [13]

Pengumpulan data dilakukan dengan mengirim e-mail yang sah dan *e-mail spoofing* dari berbagai mailer dengan target penerima dari mailer yahoo, gmail, dan hotmail. Setelah pengumpulan data dirasa cukup, tindakan selanjutnya adalah menganalisis *header e-mail* dengan mengimplementasikan langkah-langkah/algoritma yang telah diajukan oleh peneliti terdahulu guna memastikan apakah langkah- langkah tersebut masih relevan digunakan atau tidak. Disamping itu, penelitian ini akan mengajukan sebuah langkah dalam mendeteksi *e-mail spoofing* untuk melengkapi penelitian yang telah ada sebelumnya.

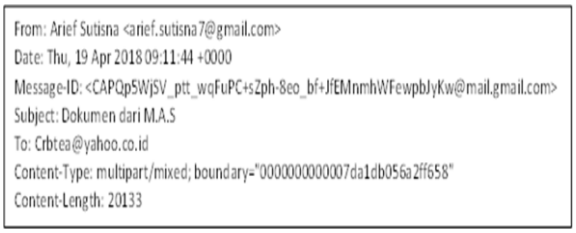
IV. Hasil dan Pembahasan

Dari pengiriman e-mail yang diterima dapat divalidasi akan kebenaran email dan *e-mail spoofing* didapat hasil sebagai berikut.

Gambar 6 Header dan Body Legitimate E-mail

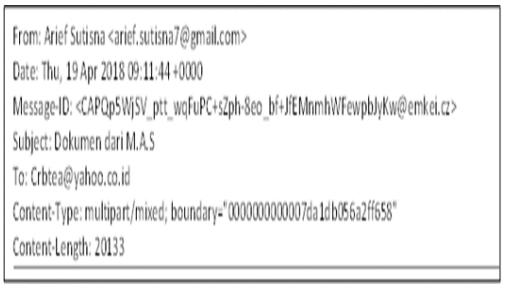
Gambar 7 *Header* dan *Body E-mail Spoofing*

Jika diperhatikan antara gambar 6 dan gambar 7 tidak ada perbedaan yang mencolok dari *legitimate* e-mail dan e-mail spoofing. Isi field yang nampak pada e-mail tersebut identik. Namun kedua e-mail tersebut datang dari alamat e-mail yang berbeda atau bahkan dari orang dan tempat yang berbeda. Ada seseorang yang mengirimkan e-mail kepada akun crbtea@yahoo.co.id atas nama yogi suhendra dengan alamat e-mail arief.sutisna7@gmail.com, Untuk dapat membuktikan keabsahan e-mail tersebut maka perlu dilakukan analisis terhadap header e-mail.



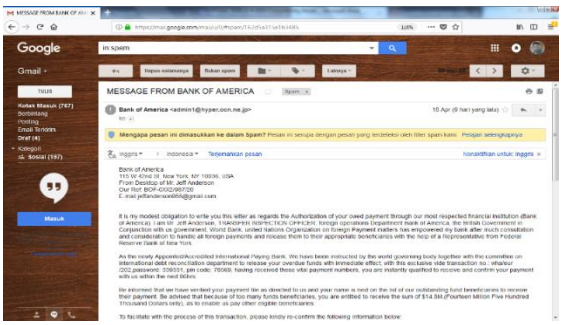
Gambar 8 *Header Legitimate E-mail*

Gambar 8 adalah *header* dari e-mail yang sah (*legitimate e-mail*). hal tersebut dapat diketahui dari keidentikan nama *domain mail server* yang berada setelah tanda @. Nama domain yang terdapat pada field '*From'* adalah gmail.com dan nama domain mail server yang terdapat pada field *'Message-ID'* adalah mail.gmail.com yang merupakan mail server dari gmail.com. karena keidentikan itulah dapat disimpulkan bahwa wmail tersebut adalah e-mail yang sah.

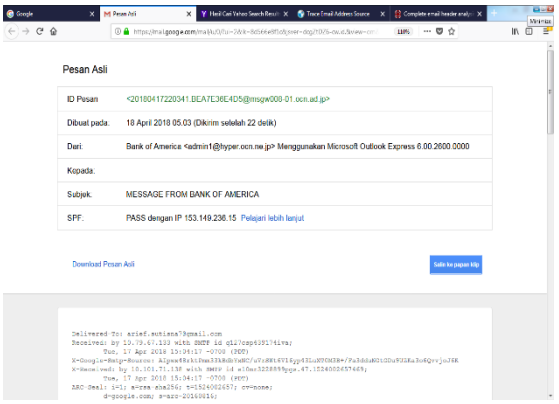


Gambar 9 *Header E-mail Spoofing*

Field 'From' mengidentifikasi alamat e-mail dari pengirim, *'Subject'* merupakan kalimat tentang isi pesan, *'To'* mengidentifikasi alamat penerima e-mail. Gambar 9 menunjukkan bahwa e-mail crbtea@yahoo.co.id menerima e-mail dari yogi suhendra dengan alamat e-mail arief.sutisna7@gmail.com dan *Subject* berisi 'Panduan Website STMIK MJ'Selanjutnya adalah *header* yang terdapat pada *e-mail spoofing,* ada ketidakcocokan nama domain mail server yang terdapat pada *field* '*From'* dan '*Message-ID'*, nama domain yang terdapat pada field '*From*' adalah gmail.com, sedangkan nama domain yang terdapat pada '*Message-ID*' adalah emkei.cz, artinya e-mail yang diterima berasal dari domain emkei.cz bukan dari gmail, karena ketidakcocokan *value* diantara kedua *field* tersebut, maka dapat diidentifikasi bahwa e-mail tersebut adalah *e-mail spoofing*.



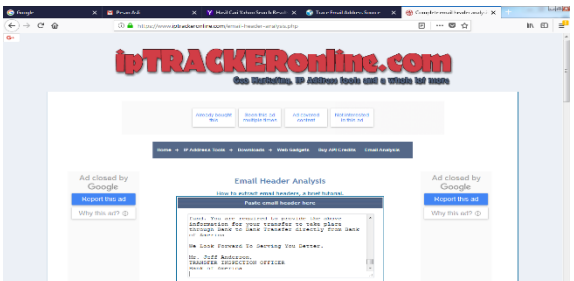
Gambar 10. *E-mail Spoofing*



Gambar 11. *Header E-mail Spoofing*

.

Blok semua tulisan dalam *header* lengkap tersebut, kemudian *copy*. Setelah itu kita menuju salah satu penyedia *email tracking online* seperti contoh penyedia *email tracking online* yang telah kita bahas diatas. Kita ambil contoh akan gunakan http://www.iptrackeronline.com/email-header-analysis.php. *Paste* kan *email header* yang telah di*copy* tadi di kotak "*paste email header here*". Dan setelah itu klik *Submit Header*.



Gambar 12. Deteksi Email Spoofing dengan Iptrackeronline

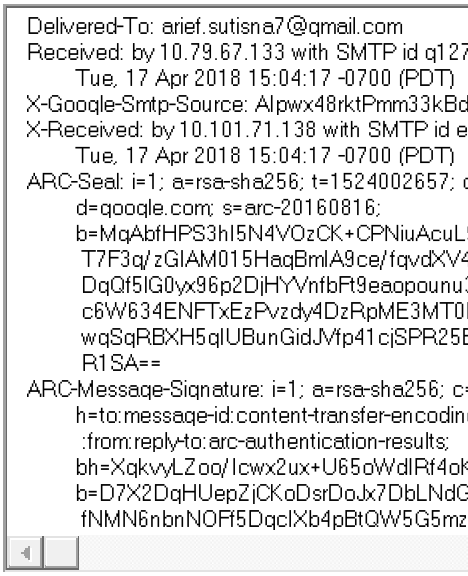
Dari hasil analisis tersebut dapat terlihat bahwa email ini dikirim dari Jepang dan sempat mampir ke beberapa account yang lain dalam Negara yang sama. Dan terlihat jelas *IP Address email* tersebut dikirim dari mana, hingga terlihat jelas lokasi peta nya.

Gambar 13. Analis *Header mail Spoofing*

Namun kekurangannya adalah, dalam lokasi peta tersebut, menurut pengamatan penulis bukan alamat asli. Namun alamat ISP tempat dikirimnya *email* tersebut.

Trace Email Analyzer

Paste the header you've copied in the box.



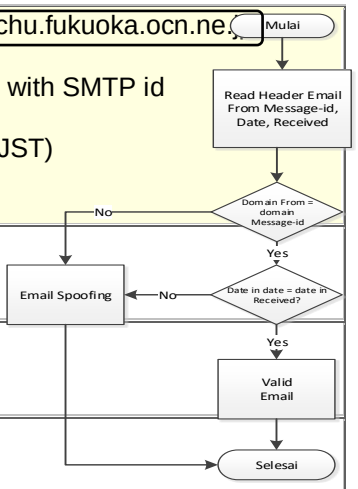
Gambar 11. Analis *Header Email Spoofing*

Delivered-To: arief.sutisna7@gmail.com	wgioLb9z Q1DAWV7SoJbPYHcZminjRdnbhkQNf9sAGdyAa64J	
Received: by 10.79.67.133 with SMTP id q127csp439174iva; Tue, 17 Apr 2018 15:04:17 -0700 (PDT)	W1I11i 90BAiJ6bQ4tMdVkrVMSfkMFvuV/J2d5eKL0zIPWe/Cb	
X-Google-Smtp-Source: AIpwx48rktPmm33kBdbYxNC/uVrSWt6V16yp43LuXT0M3B+/Pa3dduNGtGDu9U ZKa3o6QvvjoJ6K	51Lr 0N4pohNT8MSqx5q6xikJ5nxL/PrRt86RXJjKYgQKjKY IL+kC JXpw==	
X-Received: by 10.101.71.138 with SMTP id e10mr3228899pgs.47.1524002657469; Tue, 17 Apr 2018 15:04:17 -0700 (PDT)		
ARC-Seal: i=1; a=rsa-sha256; t=1524002657; cv=none; d=google.com; s=arc-20160816; b=MgAbfHPS3hI5N4VOzCK+CPNiuAcuL9Af8EKaXgN9k5pfBiXQSQkrqKcBd6C/ BYn8UK T7F3q/zGIAM015HagBmIA9ce/fqvdXV4yvGs0+Ycynh sb DqQf5lG0yx96p2DjHYVnfbFt9eaopounu3xULdxJk24o wP/R c6W634ENFTxEzPvzdy4DzRpME3MT0MnQP+f8Z8O Cy+ZE3U wgSgRBXH5qIUBunGidJVfp41cjSPR25BhxA1Wcblwf Gb/ZM R1SA==	ARC-Authentication-Results: i=1; mx.google.com; spf= of admin1@hyper.ocn.ne.jp designates 153.149.236.1 smtp.mailfrom=admin1@hyper.ocn.ne.jp Return-Path: <admin1@hyper.ocn.ne.jp>	
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=to:message-id:content-transfer-en version:date:subject :from:reply-to:arc-authentication-r bh=XqkvyLZoo/Icwx2ux+U65oWdIRf4oKBHABta32S5 b=D7X2DgHUepZjCKoDsrDoJx7DbLNdGFKrD8rt5Vm 0JXWR7 fNMN6nbnNOFf5DgcIXb4pBtQW5G5mztIQ/Z+N0So1	Received: from mbkd0314.ocn.ad.jp (mbkd0314.ocn.a mx.google.com with ESMTP id v66si6307474pfd.341. 17 Apr 2018 15:04:17 -0700 (PDT) Received-SPF: pass (google.com: domain of admin1@ Hsp4p/sBsNZrae1KlLWjgS designates 153.149.236.15 as permitted sender) clien Authentication-Results: mx.google.com; spf=pass (goo admin1@hyper.ocn.ne.jp designates 153.149.236.15 a smtp.mailfrom=admin1@hyper.ocn.ne.jp Received: from mf-smf-ucb032c2 (mf-smf-ucb032c2.o by mbkd0314.ocn.ad.jp (Postfix) with ESMTP id 1EAB 2018 07:03:59 +0900 (JST) Received: from msgw008-01.ocn.ad.jp ([180.37.203.1 with ESMTP id 8Yhjfi87HMgq48YhjfKpdi; Wed, 18 Apr	

Received: from User (p343132-ipngn200709fukuokachu.fukuoka.ocn.ne.jp [124.103.81.132]) by msgw008-01.ocn.ad.jp (Postfix) with SMTP id BEA7E36E4D5; Wed, 18 Apr 2018 07:03:41 +0900 (JST)
Reply-To: <jeffanderson955@gmail.com>
From: Bank of America <admin1@hyper.ocn.ne.jp>
Subject: MESSAGE FROM BANK OF AMERICA
Date: Tue, 17 Apr 2018 15:03:55 -0700
MIME-Version: 1.0
Content-Type: text/plain; charset="Windows-1251"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
Message-Id: <20180417220341.BEA7E36E4D5@msgw008-01.ocn.ad.jp>
To: undisclosed-recipients:;

Gambar 12. Analis *Header Email Spoofing*

Berikut *flowchart* dari deteksi *e-mail spoofing.*



Gambar 13. *Flowchart* Deteksi *E-mail spoofing*

Keterangan :

1. Membaca header e-mail khususnya *field 'From','Message-ID', 'Date',* dan *'Received'*
2. Jika nama domain yang terdapat pada *field'From'* sama dengan nama domain yang terdapat pada *field 'Message-ID'*, maka selanjutnya akan dilakukan pengecekan terhadap *field 'Date'* dan *'Received'*, jika tanggal yang terdapat pada *'Date'*sama dengan tanggal yangterdapat pada last *'Received'*, maka e-mail tersebut adalah e-mail yang sah jika tidak maka e-mail tersebut adalah *e-mail spoofing*.

E-mail spoofing terbagi tiga pola, yaitu:

1. *E-mail spoofing* secara keseluruhan seperti yang ditunjukkan oleh e-mail no. 2, artinya e-mail dikirim dengan memanipulasi alamat e-mail dan tanggal e-mail. manipulasi e-mail bisa dilihat dari membandingkan *value* yang terdapat pada *From* dan *Message-ID*, sedangkan manipulasi tanggal bisa dilihat pada *value* yang terdapat pada *Date* dan *Received (last).*
2. *E-mail spoofing* dengan memanipulasi alamat e-mailnya saja, hal tersebut ditunjukan oleh e-mail no.3 dimana nama domain server yang ada pada field From berbeda dengan nama domain yang ada pada *Message-ID*, sedangkan untuk tanggal pengiriman e-mail tidak ada

manipulasi.

3. *E-mail spoofing* dengan memanipulasi tanggal, seperti yang ditunjukkan oleh e-mail no. 5. Alamat e-mail yang tertera merupakan alamat e-mail yang sah karena domain yang dimiliki oleh *From* dan *Message-ID* memiliki *value* yang sama, namun ternyata ada manipulasi tanggal, *Date* menunjukkan tanggal 2 Oct 2016 sedangkan tanggap pada *Received* menunjukkan tanggal 2 Nov 2016. Tanggal yang sebenarnya adalah tanggal yang terdapat pada *Received*.

V. Kesimpulan dan Saran

Berdasarkan uraian yang telah dijelaskan maka dapat disimpulkan bahwa :

1. E-mail sangat mudah untuk dipalsukan untuk mengelabui korban. Bagian e-mail yang mudah dimanipulasi adalah *header* e-mail, *Field header* yang sering digunakan untuk memanipulasi adalah *From* dan *Date*. Pengelabuan atau pemalsuan ini biasa dikenal dengan istilah *e-mail spoofing.*
2. Terdapat tiga pola *e-mail spoofing*, yaitu
   a. *e-mail spoofing* yang tanggal memalsukan alamat dan e-mail,
   b. *e-mail spoofing* yang memalsukan alamat e-mailnya saja,
   c. *e-mail spoofing* yang memalsukan tanggal pengirimannya saja.
3. Pendeteksian adanya *e-mail spoofing* dapat dilakukan dengan metode header analisis dengan menggunakan *field-field* yang mengandung infomasi yang dibutuhkan seperti *From*, *Message-ID*, *Received*, *Date*,

Saran untuk peneliti selanjutnya adalah membangun sebuah aplikasi pendeteksi *e-mail spoofing* yang difungsikan sebagai *alert* yang ditanamkan pada sisi *mail client*. Pada sisi mail server, hendaknya meningkatkan keamanan dengan memberlakukan sistem *authentication* terhadap e-mail yang masuk berdasarkan ciri-ciri *e-mail spoofing* yang terdapat pada *header* e-mail.

Daftar Pustaka

[1] APJII. (2018).Penetrasi & Perilaku Pengguna Internet Indonesia 2018. From http://apjii.com

[2] Muhammad Nuh Al-Azhar (2012). Digital Forensic Panduan Praktis Investigasi Komputer. Jakarta : Salemba Infotek.

[3] Jayan, A., & S, D. (2015). Detection of Spoofed Mails. Retrieved from http://www.fraudguides.com/internet/detect-spoofed- e-mails/

[4] Gupta, S., Pilli, E. S., Mishra, P., Pundir, S., & Joshi, R. C. (2014). Forensic Analysis of E-mail Address Spoofing, 898–904.

[5] Karie, N. M., & Venter, H. S. (2014). Towards a General Ontology for Digital Forensic Disciplines, 1–29. Retrieved from https://books.google.co.id/books?isbn-1910810827

[4] Kurniawan, H. (2005). *Panduan Praktis Instalasi E-mail Server Gratis Berbasis Windows Menggunakan hMailServer*. Jakarta: PT. Elex Media Komputindo

[5] Chhabra, G. S. (2015). Review of E-mail System , Security Protocols and E-mail Forensics, *5*(3), 201–211.

[6] Devendran, V. K., Shahriar, H., & Clincy, V. (2015). A Comparative Study of E-mail Forensic Tools. *Journal of Information Security*, *06*(02),111–117. doi:10.4236/jis.2015.62012

[7] Rafiudin, R. (2009). *Investigasi Sumber-sumber Kejahatan Internet : Internet Forensics*. (N. WK, Ed.). Andi. doi:10987654321

[8] https://www.masterpendidikan.com/2017/01/10-pengertian-email-menurut-para-ahli.htm

[9] Jean-François Pillou

https://id.ccm.net/contents/21-struktur-email-header-dan-badan-email

[10] Banday, M. T. (2011). Analysing internet e-mail date spoofing, *vol.7*, 145–143. Retrieved from dl.acm.org/citation.cfm?id=2296268

[11] Chandraleka, H. (2009). *Trik Mengantisipasi Hacking E-mail*. (I. Rouf, Ed.) (1st ed.). Jakarta: mediakita.[11] Abdussalam. (2006). *Forensik*. (T. R. Agung, cle/download/791/724

Ed.).Jakarta: Restu Agung.

[12] Banday, M. T. (2011). T ECHNIQUES AND T OOLS FOR F ORENSIC I NVESTIGATION OF E- MAIL, *3*(6), 227–241. Retrieved from airccse.org/journal/nsa/1111nsa17.pdf

[13] Karsono, K.(2012). FORENSIK E-MAIL. Retrieved from http://ejurnal.esaunggul.ac.id/index.php/Formil/arti