

ANALISISA FORENSIK PADA E-MAIL SPOOFING

Mochammad Arief Sutisna¹,

Magister Teknologi Informasi, Universitas Ahmad Dahlan
Email : arief.sutisna7@gmail.com¹

Dr. Imam Riadi², M.Kom

Universitas Ahmad Dahlan

Jl. Dr. Soepomo Sh no.80, Waroengboto, Umbulharjo, Yogyakarta, Indonesia
Email : imam.riadi@mti.uad.ac.id²

Abstraksi

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

Kata Kunci :

Forensik email, Legitimate email, Email spoofing, Header Analysis

Pendahuluan

Layanan internet 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 +7,6% per Agustus 2015 [1]. Di Indonesia sendiri, internet mengalami pertumbuhan sebesar 15% mulai Januari 2015 – Januari 2016 [2],

Salah satu layanan internet yang banyak digunakan adalah email. email (*electronic mail*) merupakan surat elektronik [3] yang berbasis file teks, namun dengan perkembangan teknologi, e-mail lebih atraktif terhadap penggunaannya, tidak hanya dapat mengirim *file* teks, tapi juga dapat mengirim file audio, video, foto dan *file* ekstensi lainnya [4].

Terdapat ancaman serius mengiringi kemudahan yang diberikan oleh e-mail dengan memanfaatkan e-mail sebagai media untuk melakukan tindak kejahatan di dunia siber, karena e-mail merupakan alat transportasi utama bagi *spam* dan konten berbahaya dalam jaringan. E-mail juga merupakan sumber utama dari kebanyakan aktivitas kriminal pada internet [5]. Salah satu ancaman dari tindak kejahatan yang menggunakan email adalah *email spoofing*.

Email spoofing adalah Pengiriman e-mail yang tidak menggunakan identitas asli [6]. Banday (2011) *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 "Reply 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 *aware* terhadap e-mail yang masuk akan terjebak dalam skenario yang sudah di design oleh *scammer* [7].

Tinjauan Pustaka

Penelitian *e-mail spoofing* yang menggunakan teknik *header analysis* telah banyak dilakukan, seperti penelitian yang dilakukan oleh Joshi, Baloni, & Bank (2014)[14] dengan menganalisis *time and date of e-mail spoofing* dengan memanfaatkan kebijakan (*policy*) yang terdapat pada server SMTP untuk memeriksa e-mail yang masuk terlebih dahulu dengan melihat *date and time* yang terdapat pada *header e-mail*. Penelitian serupa juga dilakukan oleh Mishra, Pilli, & Joshi (2012) yang melakukan penelitian terhadap *e-mail spoofing* dengan membandingkan waktu pengiriman e-mail (*sending time*) dan waktu penerimaan pesan (*last server email receiving time*).

Penelitian lain juga dilakukan oleh Wahyudi (2008). Penelitian dilakukan terhadap *email 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 email. Teknik analisis *header e-mail spoofing* juga dapat dilakukan dengan menganalisis alamat pengirim e-mail. selanjutnya Jayan & S (2015) juga mengusulkan teknik analisis *header e-mail* terhadap *time and date* yang difokuskan pada komponen *received*. Penelitian yang dilakukan oleh peneliti tersebut berfokus pada tanggal pengiriman dan penerimaan e-mail.

Berdasarkan referensi dari penelitian terdahulu, maka penelitian ini bertujuan untuk mengetahui bagaimana mengidentifikasi status keabsahan sebuah email berdasarkan tanggal dan alamat sebuah email sebagai wujud kombinasi dari hasil peneliti yang pernah dilakukan oleh peneliti lain. Teknik investigasi yang akan digunakan dalam penelitian ini adalah teknik *header analysis* dengan menggunakan field 'From', 'Message-ID', 'Date', dan 'Received' sebagai parameter deteksi *email spoofing*.

Forensik

Forensik berasal dari bahasa Latin yaitu forensis yang berarti "dari luar", dan memiliki pengertian bidang ilmu pengetahuan yang digunakan untuk membantu proses penegakan keadilan melalui proses penerapan ilmu dan sains. Abdussalam (2006) menyatakan bahwa Forensik merupakan alat bukti sah dalam memberikan keyakinan hakim untuk

memutuskan tersangka/terdakwa bersalah dan/atau tidak bersalah [11]. Forensik sendiri terbagi menjadi beberapa jenis ilmu forensik dari berbagai bidang disiplin ilmu seperti *medicine forensics, fisika forensics, chemistry forensics, balistik metallurgy forensics, document forensics, computer/digital forensics, dan sebagainya*.

Digital Forensics

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)

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*.

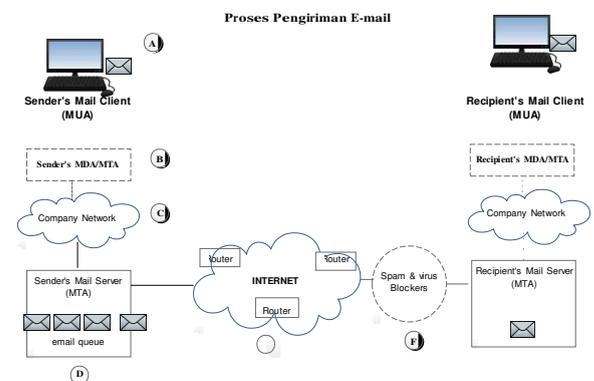
Internet Forensics

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). Salah satu fasilitas internet yang banyak digunakan adalah email.

Email

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.

Pasapatheeswaran (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 [17].



Gambar 1 Alur Proses Pengiriman Email

Header Email

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

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

Kejahatan yang melibatkan email

Kejahatan yang melibatkan email antara lain; *Spamming* adalah pesan komersial yang tidak diminta (*bulk email*). *E-mail worm* adalah email yang digunakan sebagai jalan untuk menggandakan dirinya ke banyak komputer. Kombinasi *spam* dan *worm* dapat sangat mengganggu *user-user* e-mail.

Email spoofing merupakan bagian dari bentuk pemalsuan. Pesan-pesan e-mail yang dikirimkan dengan sengaja dipalsukan supaya tampak seolah-olah dari alamat e-mail yang sah (*legitimate email*). *Email spoofing* seringkali ditempuh dengan mengubah *header-header* e-mail. *E-mail bombing* adalah usaha mentransfer e-mail dalam jumlah ekstra besar ke sebuah target (*email address*), sehingga *account* email korban mengalami *crash* atau tidak dapat digunakan lagi.

Email Forensics

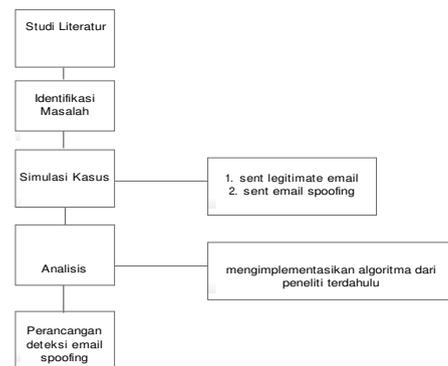
Banday (2011) dalam penelitiannya menyatakan bahwa *e-mail forensics* mengacu pada studi tentang sumber dan isi email sebagai alat bukti untuk mengidentifikasi pengirim email yang sebenarnya dan penerima email, tanggal / waktu ketika email ditransmisikan, *detail record* tentang transaksi email [8]. untuk dapat melakukan *e-mail forensics* terdapat beberapa teknik investigasi dalam melaksanakannya, sedangkan menurut Karsono (2012) forensik e-mail adalah suatu tindakan pengamanan, pengecekan, serta penelusuran terhadap email palsu atau terhadap

bukti-bukti kejahatan yang menggunakan e-mail [9]. Pengertian e-mail forensik juga disampaikan oleh Devendran et al (2015) bahwa pemeriksaan dan pengungkapan informasi penting yang terdapat pada e-mail merupakan aktivitas *e-mail forensics* [10].

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).

Metode Penelitian



Gambar 2 Alur Deteksi Email Spoofing

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 email*,

Pengumpulan data dilakukan dengan mengirim email yang sah dan *email spoofing* dari berbagai mailer dengan target penerima dari mailer yahoo, gmail, dan hotmail. Setelah pengumpulan data dirasa cukup, tindakan selanjutnya adalah menganalisis *header email* 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 *email spoofing* untuk melengkapi penelitian yang telah ada sebelumnya.

Hasil dan Pembahasan

Dari pengiriman email yang sah (*legitimate email*) dan *email spoofing* didapat hasil sebagai berikut.



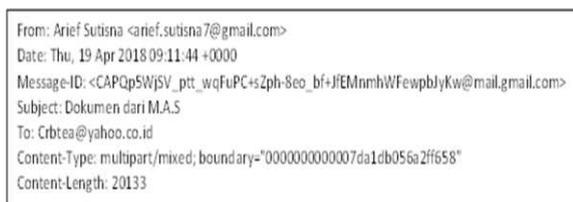
Gambar 3 Header dan Body Legitimate Email

Field 'From' mengidentifikasi alamat email dari pengirim, 'Subject' merupakan kalimat tentang isi pesan, 'To' mengidentifikasi alamat penerima email. Gambar 1 menunjukkan bahwa email crbtea@yahoo.co.id menerima email dari yogi suhendra dengan alamat email arief.sutisna7@gmail.com dan Subject berisi 'Panduan Website STMIK MJ'



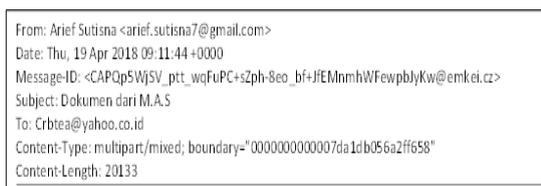
Gambar 4 Header dan Body Email Spoofing

Jika diperhatikan antara gambar 3 dan gambar 4 tidak ada perbedaan yang mencolok dari legitimate email dan email spoofing. Isi field yang nampak pada email tersebut identik. Namun kedua email tersebut datang dari alamat email yang berbeda atau bahkan dari orang dan tempat yang berbeda. Ada seseorang yang mengirimkan email kepada akun crbtea@yahoo.co.id atas nama yogi suhendra dengan alamat email arief.sutisna7@gmail.com, Untuk dapat membuktikan keabsahan email tersebut maka perlu dilakukan analisis terhadap header email.



Gambar 5 Header Legitimate Email

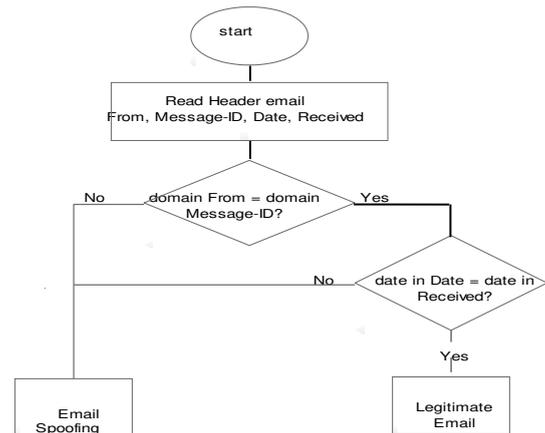
Gambar 5 adalah header dari email yang sah (legitimate email). hal tersebut dapat diketahui dari keidentikan nama domain mail server yang berada setelah tanda @. Nama domain yang terdapat pada field 'From' adalah gmail.com dan nama domain mail server yang terdapat pada field 'Message-ID' adalah mail.gmail.com yang merupakan mail server dari gmail.com. karena keidentikan itulah dapat disimpulkan bahwa wmail tersebut adalah email yang sah.



Gambar 6 Header Email Spoofing

Selanjutnya adalah header yang terdapat pada email 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 email yang diterima berasal dari domain emkei.cz bukan dari gmail, karena ketidakcocokan value diantara kedua field tersebut, maka dapat diidentifikasi bahwa email tersebut adalah email spoofing.

Berikut flowchart dari deteksi email spoofing.



Gambar 7 Flowchart Deteksi Email spoofing

Jika dituangkan dalam sebuah algoritma, maka hasilnya adalah sebagai berikut:

```

while (email header are available)
{
    read header email From, Message-ID,
    Date, Last Received
    if (domain from = domain Message-ID)
    {
        If (date in Date = date in
        Received)
        {
            //legitimate email
        }
    }
    else
    {
        //email date spoofing
    }
}
else
{
    //email spoofing
}
}
    
```

Gambar 8 Algoritma Deteksi Email Spoofing

Keterangan :

1. Membaca header email 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 yang

terdapat pada last 'Received', maka email tersebut adalah email yang sah jika tidak maka email tersebut adalah *email spoofing*.

email spoofing terbagi tiga pola, yaitu:

1. *Email spoofing* secara keseluruhan seperti yang ditunjukkan oleh email no. 2, artinya email dikirim dengan memanipulasi alamat email dan tanggal email. manipulasi email 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. *Email spoofing* dengan memanipulasi alamat emailnya saja, hal tersebut ditunjukkan oleh email no.3 dimana nama domain server yang ada pada field *From* berbeda dengan nama domain yang ada pada *Message-ID*, sedangkan untuk tanggal pengiriman email tidak ada manipulasi.
3. *Email spoofing* dengan memanipulasi tanggal, seperti yang ditunjukkan oleh email no. 5. Alamat email yang tertera merupakan alamat email 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 tanggal pada *Received* menunjukkan tanggal 2 Nov 2016. Tanggal yang sebenarnya adalah tanggal yang terdapat pada *Received*.

Kesimpulan dan Saran

Berdasarkan uraian yang telah dijelaskan maka dapat disimpulkan bahwa :

1. Email rentan dan sangat mudah untuk dipalsukan untuk mengelabui korban. Bagian email yang mudah dimanipulasi adalah *header* email, *Field header* yang sering digunakan untuk memanipulasi adalah *From* dan *Date*.

Pengalabuan atau pemalsuan ini biasa dikenal dengan istilah *email spoofing*.

2. Terdapat tiga pola *email spoofing*, yaitu : 1) *email spoofing* yang memalsukan alamat dan tanggal email, 2) *email spoofing* yang memalsukan alamat emailnya saja, 3) *email spoofing* yang memalsukan tanggal pengirimannya saja.
3. Pendeteksian adanya *email spoofing* dapat dilakukan dengan metode header analisis dengan menggunakan *field-field* yang mengandung informasi yang dibutuhkan seperti *From*, *Message-ID*, *Received*, *Date*,

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

Daftar Pustaka

- [1] Wearesocial. (2015). Digital, Social & Mobile in 2015. Retrieved from <http://wearesocial.com/sg/special-reports/digital-social-mobile-2015>
- [2] Liputan6. (2016). Seorang Wanita Ditangkap karena Menipu Pengusaha HP dengan Modus E-mail Spoofing. Retrieved from www.detik.com/news/berita/2807748/Seorang-Wanita-Ditangkap-karena-Menipu-Pengusaha-HP-dengan-Modus-E-mail-Spoofing
- [3] Kurniawan, H. (2005). *Panduan Praktis Instalasi E-mail Server Gratis Berbasis Windows Menggunakan hMailServer*. Jakarta: PT. Elex Media Komputindo

- [4] Chhabra, G. S. (2015). Review of E-mail System , Security Protocols and Email Forensics, *5*(3), 201–211.
- [5] Devendran, V. K., Shahriar, H., & Clincy, V. (2015). A Comparative Study of Email Forensic Tools. *Journal of Information Security*, *06*(02), 111–117. doi:10.4236/jis.2015.62012
- [6] Gupta, S., Pilli, E. S., Mishra, P., Pundir, S., & Joshi, R. C. (2014). Forensic Analysis of E-mail Address Spoofing, 898–904.
- [7] Banday, M. T. (2011). Analysing internet e-mail date spoofing, *vol.7*, 145–143. Retrieved from dl.acm.org/citation.cfm?id=2296268
- [8] 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
- [9] Karsono, K. (2012). FORENSIK E-MAIL. Retrieved from <http://ejurnal.esaunggul.ac.id/index.php/Formil/article/download/791/724>
- [10] Chandraleka, H. (2009). *Trik Mengantisipasi Hacking Email*. (I. Rouf, Ed.) (1st ed.). Jakarta: mediakita.
- [11] Abdussalam. (2006). *Forensik*. (T. R. Agung, Ed.). Jakarta: Restu Agung.
- [12] Ghawate, T., Patel, C., Bargaje, R., Kadam, K., & Khanuja, P. H. (2015). Security Suite, *4*(3).
- [13] Jayan, A., & S, D. (2015). Detection of Spoofed Mails. Retrieved from www.fraudguides.com/internet/detect-spoofed-emails/
- [14] Joshi, N., Baloni, D., & Bank, K. (2014). COUNTER-MEASURES TO PREVENT SPOOF E-MAIL TRACKING Abstract :, (Iocrsem), 91–98.
- [15] Karie, N. M., & Venter, H. S. (2014). Towards a General Ontology for Digital Forensic Disciplines, 1–29. Retrieved from www.ncbi.nlm.nih.gov/pubmed/24931294
- [16] Mishra, P., Pilli, E. S., & Joshi, R. C. (2012). Forensic Analysis of E-mail Date and Time Spoofing, 309–314. doi:10.1109/ICCCT.2012.69
- [17] Pasupatheeswaran, S. (2008). Email ' Message-IDs 'helpful for forensic analysis ? Retrieved from ro.ecu.edu.au/cgi/viewcontent.cgi?article=1048&context=adf
- [18] Rafiudin, R. (2009). *Investigasi Sumber-sumber Kejahatan Internet : Internet Forensics*. (N. WK, Ed.). Andi. doi:10987654321
- [19] Wahyudi, M. D. R. (2008). Deteksi e-mail palsu dengan mempergunakan. *Jurnal Teknologi*, *1*, 119–126. Retrieved from http://jurtek.akprind.ac.id/sites/default/files/119_12_6_Didik.pdf