ISSN: 2087-1716
ILKOM Jurnal Ilmiah Volume 8 Nomor 3 (Desember 2016)

ANALISIS LIVE FORENSICS UNTUK PERBANDINGAN KEMANANAN EMAIL PADA SISTEM OPERASI PROPRIETARY

Muhammad Nur Faiz[1], Rusydi Umar[2], Anton Yudhana[3]
[1]hafarafaiz@gmail.com, [2]rusydi@live.in, [3]eyudhana@ee.uad.ac.id
[1,2,3]Universitas Ahmad Dahlan,

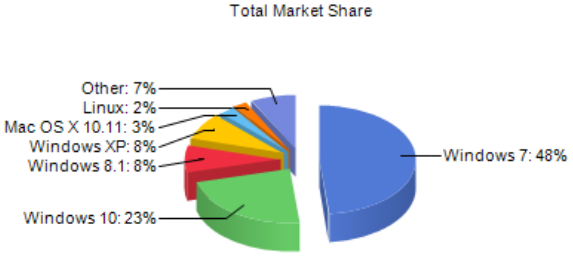
Abstrak

Email menjadi salah satu media untuk berkomunikasi dan bisa menyimpan bukti kejahatan, saat ini telah banyak kejahatan yang terjadi melalui media ini. *Digital forensics* merupakan salah satu ilmu untuk menemukan barang bukti termasuk *email* sebagai bukti digital. Analisis digital forensik terbagi menjadi dua, yaitu tradisional / *dead* dan *live forensics*. Analisis *forensics* tekni digital tradisional menyangkut data yang disimpan secara permanen di perangkat, sedangkan analisis *live forensics* yaitu analisis menyangkut data sementara yang disimpan dalam peralatan atau *transit* di jaringan. jurnal ini mengusulkan analisis *forensics live* di sistem operasi terbaru yaitu Windows 10. Studi kasus berfokus pada kemanan beberapa *email* seperti Gmail, Yahoo dan Outlook dan beberapa *browser* secara umum seperti Google Chrome, Mozilla Firefox, dan Microsoft Edge. Hasil Eksperimen penelitian ini yaitu masing-masing penyedia *email* menambahkan fitur tersendiri demi keamanan user.

Kata kunci: Digital Forensics, live forensics, Email, Browser.

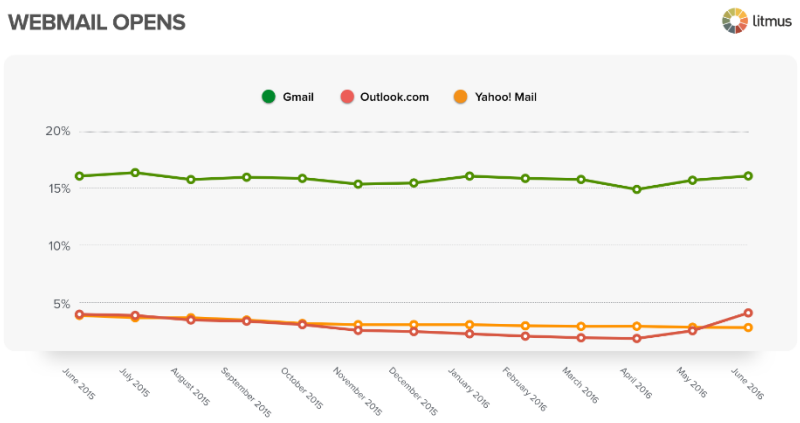
1. Pendahuluan

Pada era informasi saat ini penggunaan *email* selain sebagai alat untuk mengirim dan menerima pesan juga sebagai alat untuk menyimpan informasi rahasia karena email terhubung dengan berbagai akun media sosial saat ini. Kejahatan akun email saat ini bertambah banyak dari tahun ke tahun seiring jumlah penggunanya yang semakin bertambah. Kejahatan *email* dapat diminimalisir dengan penggunaan username dan *password* yang rumit, selain itu teknik *hacking* yang mulai meningkat seiring dengan penggunaan *tools* yang *freeware* menyebabkan penyalahgunaan *email* menjadi lebih banyak. *Digital forensics* sabagai suatu ilmu untuk menemukan barang bukti dari kejahatan yang telah terjadi yang *valid* atau dapat dipertanggungjawabkan di pengadilan. *Digital forensics* ini dibagi menjadi dua teknik yaitu *live forensics* dan *dead forensics*. Teknik *live forensics* ini sangat bergantung pada keadaan komputer yang sedang menyala, karena membutuhkan data yang berjalan pada *Random Access Memory* (RAM). Data pada RAM disebut juga *data volatile* atau data sementara yaitu data yang hanya terdapat saat komputer menyala jika komputer mati maka data itu akan hilang. *Data volatile* ini berisi data penting seperti *username*, *password*, file akses, file modifikasi, aplikasi yang digunakan, kata kunci pencarian. *Username* dan *password* merupakan hal yang penting dalam suatu akun seperti *email*. *Email* ini biasanya mengirimkan sesuatu yang penting bahkan data privasi suatu perusahaan atau penggunanya. Konsep perusahaan sekarang ini dengan menerapkan *virtual office* yaitu perusahaan yang tidak ada kantor hanya melayani konsumen dengan media online, oleh karena itu pengguna email semakin tahun semakin bertambah dengan konsep virtual ini. Untuk menjalankan email dibutuhkan jaringan internet, browser dan sistem operasi. Sistem operasi terbagi menjadi dua yaitu sistem operasi *open source* dan sistem operasi *proprietary*. Sistem operasi *proprietary* ini merupakan sistem operasi yang banyak digunakan oleh perusahaan atau seseorang di seluruh dunia. Sistem operasi Windows 10 merupakan sistem operasi terbaru versi ke 18 dari Microsoft yang diperkenalkan April 2015. Versi Windows 10 merupakan versi pengembangan dari Windows 8.1 dimana Windows 10 ini terkenal dengan *cortana* yaitu sebagai *assistant* untuk membantu kinerja dari penggunanya.



Gambar 1. Jumlah Pengguna Sistem Operasi seluruh dunia Oktober 2016 [1]

Dari gambar di atas dapat dilihat bahwa jumlah pengguna Windows 7 terbanyak di dunia dengan nilai 48% hamper setengah dari jumlah pengguna sistem operasi di dunia. Sedangkan Windows 10 berada pada peringkat dua yaitu dengan 23% dari seluruh pengguna sistem operasi di dunia. Windows XP dan Windows 8.1 bernilai sama yaitu 8% dan Mac OS X 10.11 yaitu 3% . pengguna Linux 2% dan 7% untuk pengguna sistem operasi lainnya. Hal ini membuktikan bahwa Windows masih menguasai pasaran sistem operasi di dunia saat ini yaitu Windows 7 dan Windows 10.



Gambar 2. Grafik pengguna webmail open dari juni 2015 sampai dengan juni 2016 [2]

Dari data yang diperoleh *Litmus Email Analytics* dari bulan Juni 2015 sampai dengan Juni 2016 Webmail open dengan jumlah pengguna terbanyak yaitu Gmail jika dibandingkan dengan Outlook dan Yahoo mail yaitu sebesar 16% dan jumlah pengguna gmail ini tergolong stabil. Webmail Outlook sendiri mengalami kenaikan dari bulan May 2016 sampai Juni 2016 yaitu mengalamai kenaikan sebesar 4.12%, hal ini akibat dari Windows akun yang masuk pada Outlook. Sedangkan pada webmail Yahoo mengalami penurunan tetapi turun tidak terlalu drastis.

Penggunaan *Email* dengan kebutuhan manusia yang terus meningkat mengakibatkan pertumbuhan email dari tahun ke tahun terus bertambah sehingga lebih terbuka dalam tindak kejahatan dari *email* seperti *spam, phising* dan *bomb*. Akun *email* merupakan suatu hal wajib dalam membuat akun media sosial sehingga bertambah setiap tahunnya.

	2015	2016	2017	2018	2019
Worldwide Email Accounts (M)	**4,353**	**4,626**	**4,920**	**5,243**	**5,594**
%Growth		*6%*	*6%*	*7%*	*7%*
Worldwide Email Users* (M)	**2,586**	**2,672**	**2,760**	**2,849**	**2,943**
% Growth		*3%*	*3%*	*3%*	*3%*
Average Accounts Per User	1.7	1.7	1.8	1.8	1.9

Gambar 3. Akun Email Seluruh Dunia dan Prakiraan Pengguna (M), 2015-2019 [1]

Dari gambar di atas dapat dilihat bahwa jumlah akun *email* di seluruh dunia diperkirakan akan terus tumbuh pada kecepatan yang sedikit lebih cepat dari jumlah pengguna *email* di seluruh dunia, terutama akun *email* konsumen, karena banyak konsumen cenderung memiliki beberapa akun *email*. Hal ini jelas menimbulkan banyak akun email yang menjadi *virtual email* atau hanya memesan sebuah *email* tetapi bisa digunakan dimasa yang akan datang dan memesan berarti telah mempersiapkan ruang atau *database* tersendiri untuk akun tersebut.

Lalu lintas *email* setiap hari akan meningkat akibat dari jumlah akun *email* yang semakin bertambah. Jasa penyedia *email* ini lebih sibuk dan membutuhkan karyawan untuk melayani para pengguna *email* yang sedang mengalami kendala dalam menggunakan *email* termasuk melayani keamanan *email* pengguna.

Daily Email Traffic	2015	2016	2017	2018	2019
Total Worldwide Emails Sent/Received Per Day (B)	205.6	215.3	225.3	235.6	246.5
% Growth		*5%*	*5%*	*5%*	*5%*
Business Emails Sent/Received Per Day (B)	112.5	116.4	120.4	124.5	128.8
% Growth		*3%*	*3%*	*3%*	*3%*
Consumer Emails Sent/Received Per Day (B)	93.1	98.9	104.9	111.1	117.7
% Growth		*6%*	*6%*	*6%*	*6%*

,

Gambar 4. Lalu Lintas Email Setiap Hari 2016-2019 [1]

Pada 2015, jumlah *email* yang dikirim dan diterima per total hari selama 205 miliar. Angka ini diperkirakan akan tumbuh tiap tahunnya rata-rata 5% selama empat tahun berikutnya, mencapai lebih dari 246 miliar pada akhir 2019. Lalu lintas email ini akan berpengaruh pada kecepatan suatu jaringan *Internet*. Untuk bisnis 112.5 miliar sedangkan untuk konsumen 93.1 miliar pada tahun 2015 dan untuk kenaikan setiap tahunnya, lalu lintas *email* bisnis sebesar 3% yaitu sekitar 4 miliar sedangkan untuk lalu lintas *email* konsumen sebesar 6% atau sekitar 6 miliar.

Dari gambar 1,2,3 dapat disimpulkan bahwa sistem operasi windows merupakan sistem operasi dengan jumlah pengguna terbanyak di dunia dan Windows 10 pada peringkat 2 yaitu sebesar 23%. Sedangkan *email* merupakan hal yang wajib dalam suatu perusahaan atau individu dan akan selalu bertambah setiap tahunnya dari jumlah penggunaan dan lalu lintas untuk setiap harinya, oleh karena itu dibutuhkan suatu penelitian yang bisa mengetahui keamanan suatu *email* dari Gmail,Ymail dan Outlook dengan metode *live forensics* sehingga pengguna akan lebih mengetahui *email* dengan fitur kemanan terbaik pada sistem operasi Windows 10.

2. Landasan Teori

Digital forensics pada intinya adalah menemukan bukti digital bisa tersimpan pada penyimpanan computer sementara, penyimpanan permanen, USB, CD, lalu lintas jaringan, dan lainnya. *Digital forensic* kemudian berkembang menjadi sesuatu yang penting dalam keamanan informasi. Keterlibatan suatu perangkat atau media dalam kejahatan computer dibedakan menjadi tiga yaitu :

- Komputer menjadi tujuan
- Komputer menjadi sarana untuk membuat kejahatan
- Komputer berfungsi menyimpan segala informasi yang mengandung tindak pidana [3]. Analisis *digital forensics* umumnya ada dua, yakni *dead forensic* dan *live forensic*. *Dead forensic* merupakan suatu teknik yang membutuhkan data yang disimpan secara permanen dalam perangkat media penyimpanan umumnya hardisk. *Live forensic* yaitu suatu teknik analisis dimana menyangkut data yang berjalan pada sistem atau *data volatile* yang umumnya tersimpan pada *Random Access Memory* (RAM) atau *transit* pada jaringan [4].

Live forensics dapat dilakukan ketika sistem belum mati atau *down*, karena hampir kesuluruhan penggunaan sistem tersimpan pada RAM, *pagefile, hibernation file* dan *crash dump file* [5] [6]. Tujuan pentingnya analisis data pada RAM, yaitu dapat mengetahui letak data tersebut dan isi data tersebut. Semua data pada komputer yang berpergian harus melewati RAM, apakah itu membutuhkan jaringan *Internet*, menyalin atau memindahkan *file*, membuka *file* pada hardisk ataupun menghapusnya semua terekam pada RAM. Perbedaaan RAM dan Hardisk yaitu RAM mencatat sesuatu yang terjadi pada waktu dan kondisi tertentu sedangkan hardisk hanya memberikan informasi data yang secara umum. Hal ini sangat penting karena hanya ada data dengan jumlah yang besar dan tidak pernah terdaftar pada hardisk yaitu data *Internet* [7] [8] [9].

Digital forensics berkaitan dengan lalu lintas internet, internet sebagai media untuk mendapatkan dan sekaligus untuk pertukaran informasi sangat rentan dengan penyalahgunaan informasi. Era *big data* saat ini membuat data informasi sangatlah rentan dengan kejahatan termasuk pada *email*. Kejahatan yang terjadi pada email umumnya adalah *phising, bomb,* dan *fraud*. Saat ini, *email* merupakan hal yang wajib bagi para pengguna *smartphone*, komputer, tablet dan yang lainnya, *email* berguna untuk memudahkan manusia berkomunikasi. *Email* menyediakan komunikasi dengan biaya yang murah, mudah, dan dapat dipercaya di seluruh dunia. Pesan email dapat berupa data teks yang dapat dibaca, gambar-gambar yang disisipkan didalamnya, *file-file* suara, dan elemen-elemen lainnya.

Pesan-pesan e*mail* ini dapat dengan mudah dibaca atau diubah oleh *user* yang tidak berhak jika metode pengamanan tambahan tidak disertakan di dalamnya [10].

Berhubungnya antara sistem informasi dengan internet membuka peluang adanya kejahatan pada jaringan komputer. Hal ini membuat penegak hukum untuk bertindak dan menangani suatu kejahatan. Hukum dari sebagian besar negara di dunia belum menjangkau daerah *cyberspace*. Saat ini hampir semua negara di dunia berlomba-lomba untuk menyiapkan landasan hukum bagi *Internet* [11].

3. Metode

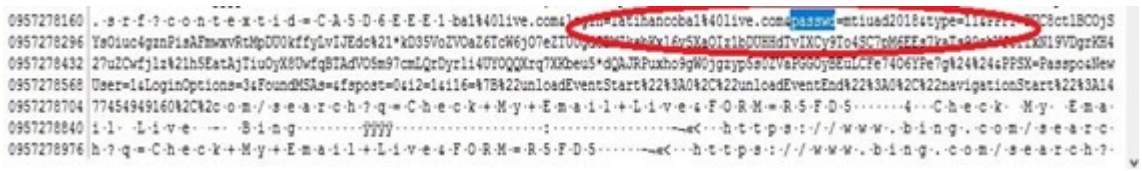
Berdasarkan penelitian yang dilakukan oleh Ellick M. Chan maka peneliti akan menggunakan metodologi penelitian The U.S. National Institute of Justice (NIJ) yang digambarkan dengan alur sebagai berikut :

Gambar 5. Metode Tahapan Digital Forensics

Metode Tahapan *Digital Forensics* seperti pada gambar diawali dengan identifikasi merupakan suatu tindak kejahatan, kemudian *collection* yaitu mengumpulkan barang bukti termasuk *imaging*, langkah selanjutnya yaitu *examination* adalah proses dimana hasil imaging diuji kebenaranya, apakah sama persis dengan data yang pertama kali imaging, kemudian langkah analisis yaitu langkah untuk mengetahui keseluruhan apa yang telah diperbuat oleh pengguna, hal apa saja yang dikatakan menyimpang dan langkah terakhir yaitu *reporting* atau laporan yaitu melaporkan dan menjelaskan apa yang telah dianalisis kemudian dipaparkan barang bukti yang telah ditemukan dan didokumentasikan secara rinci.

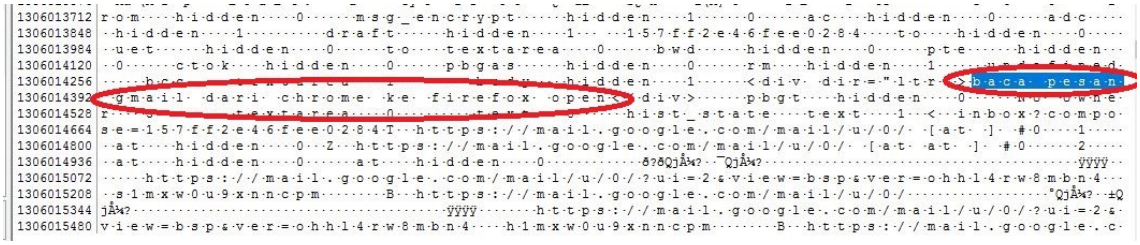
4. Hasil

Hasil ekperimen yang dilakukan dengan menggunakan *Personal Computer* Sistem Operasi Windows 10 64bit, *browser* Mozilla Firefox 49.0.1, Microsoft Edge 20.10240.17146.0, Google Chrome 54.0.2840.59, *capture* dan analisis pada FTK Imager 3.4.2.6. Penelitian ini juga membuat akun *email* latihancoba1@gmail.com *login* pada Google Chrome, latihancoba1@yahoo.com *login* pada Mozilla Firefox , latihancoba1@live.com *login* pada Microsoft Edge.



Gambar 6. Microsoft Edge *type public* pada *email* Outlook terlihat *username* dan *password*

Dari Gambar 6 menunjukkan bahwa Microsoft Edge dengan *type public* pada Outlook terlihat dengan jelas *username* dan *password* yaitu dengan *username* latihancoba1@live.com dan *password* mtiuad2016.

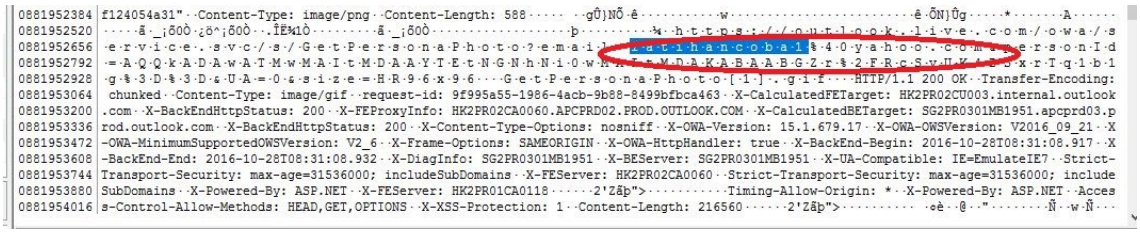


Gambar 7. Google Chrome *type public* pada *email* Gmail terlihat isi *email*

Dari Gambar 7 menunjukkan bahwa Google Chrome dengan *type public* pada Gmail terlihat dengan jelas isi pesan yang dikirimkan yaitu baca pesan Gmail dari chrome ke firefox open.

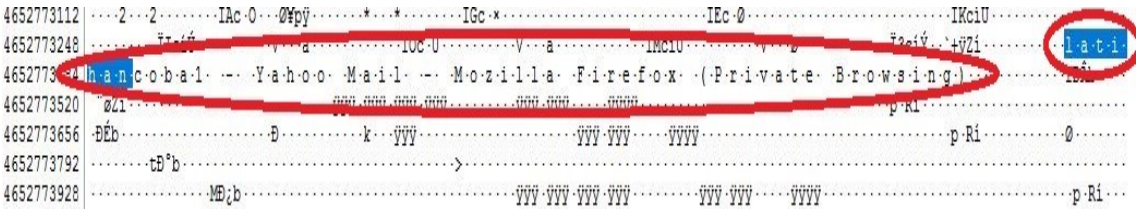
Gambar 8. Google Chrome *type public* pada *email* Gmail terlihat *subject email*

Dari Gambar 8 menunjukkan bahwa Mozilla Firefox dengan *type public* pada Yahoo terlihat dengan jelas *subject* pesan *email* yang dikirimkan yaitu kasus_open1.



Gambar 9. Microsoft Edge *type private* pada *email* Outlook terlihat kontak

Dari Gambar 9 menunjukkan bahwa Microsoft Edge dengan *type private* pada Outlook masih dapat dilihat kontak *email* yaitu latihancoba1@yahoo.com.



Gambar 10. Mozilla Firefox *type private* pada *email* yahoo terlihat *username*

Dari Gambar 10 menunjukkan bahwa Mozilla Firefox dengan *type private* pada yahoo masih dapat dilihat *username* yaitu latihancoba1.

Tabel 1. Hasil Perbandingan *Email*

Email	Type Browser	Username	Recepient	Body	Subject	Password
Outlook	Public	Yes	No	No	No	Yes
Yahoo	Public	Yes	No	No	No	Yes
Email	**Type Browser**	**Username**	**Recepient**	**Body**	**Subject**	**Password**
Outlook	Private	Yes	Yes	No	No	No
Yahoo	Private	Yes	No	No	No	No
Gmail	Private	No	No	No	No	No

Dari tabel 1 dapat dilihat bahwa untuk *type public* dengan *email* Outlook, Yahoo dan Gmail *username* masih dapat terlihat sedangkan untuk penerima atau *recipient, body* dan *subject* email hanya Gmail yang hanya dapat dilihat sedangkan untuk *password* sebaliknya yaitu hanya Gmail yang hanya tidak terlihat. Untuk *type private username* hanya dapat terlihat pada Outlook dan Yahoo sedangkan Gmail tidak, untuk *recipient* hanya terlihat pada *browser* Outlook, Email yang lain tidak terlihat. Untuk *body, subject* dan *password* semua *email* dengan *type private* tidak terlihat.

5. Kesimpulan dan saran

5.1. Kesimpulan

Email merupakan hal pendukung kinerja suatu perusahaan atau penggunanya dalam segala bidang termasuk untuk bisnis dan bertukar informasi. *Email* ini merupakan akun yang terintegrasi dengan akun sosial media lain untuk itu harus terjaga keamanannya. Metode *live forensics* merupakan suatu teknik untuk menemukan barang bukti pada *data volatile* termasuk *username* dan *password*. Jasa penyedia *email* terus berkembang dengan menambahkan berbagai fitur demi kenyamanan pengguna termasuk fitur kemanan. Gmail sebagai penyedia *email* no 2 di dunia saat ini sangatlah dibutuhkan keamanan yang tinggi dan jika dibandingkan dengan Outlook dan Yahoo, gmail merupakan *email* terbaik saat ini dengan dukungan keamanan yang tinggi pada *mode browser private*.

5.2. Saran

1. Membandingkan antara sistem operasi
2. Membandingkan akun media sosal lain
3. Menggunakan tools digital forensics lain

Daftar Pustaka

[1] Netmarketshare, “Desktop Operating System Market Share,” 2016. waktu akses 20 November 2016

[2] J. Jordan, “Mobile, Webmail + Desktop Email Market Share Trends for the 1st Half of 2016,” 2016. waktu akses 20 November 2016

[3] F. Gianni and F. Solinas, “Live digital forensics: Windows XP vs Windows 7,” *IEEE*, pp. 1–6, 2013.

[4] R. Umar, A. Yudhana, and M. N. Faiz, “ANALISIS KINERJA METODE LIVE FORENSICS UNTUK INVESTIGASI RANDOM ACCESS MEMORY PADA SISTEM PROPRIETARY,” in *Prosiding Konferensi Nasional Ke- 4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM)*, 2016, pp. 207–211.

[5] N. Joseph, S. Sunny, S. Dija, and K. L. Thomas, “Volatile Internet evidence extraction from Windows systems,” *2014 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2014*, 2015.

[6] B. D. Carrier, “Digital forensics works,” *IEEE Secur. Priv.*, vol. 7, no. 2, pp. 26–29, 2009.

[7] E. M. Chan, “A FRAMEWORK FOR LIVE FORENSICS,” University of Illinois at Urbana-Champaign, 2011.

[8] M. H. Ligh, A. Case, J. Levy, and Aa. Walters, *The Art of Memory Forensics*. Indianapolis: simultaneously, 2014.

[9] M. H. Ligh, S. Adair, B. Hartstein, and M. Richard, *Malware Analyst’s Cookbook*. Indianapolis: Wiley Publishing, Inc., 2011.

[10] A. Surachman, “Aplikasi Web 1.0.: E-mail – Surat Elektronik 1,” 2009.

[11] B. Rahardjo, *Berbasis Internet*, vol. 0. 1999.