JISKa, Vol. 1, No. 3, Januari, 2017, Pp. 108 – 114
ISSN 2527 -5836

Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email

Muhammad Nur Faiz [(1)], Rusydi Umar [(2)], Anton Yudhana [(3)]
Program Studi Magister Teknik Informatika
at Jl. Prof. Dr. Soepomo, S.H. Janturan Yogyakarta
e-mail : hafarafaiz@gmail.com

Abstract

Digital Forensics become one popular term because Currently many violations of cyber crime. Digital techniques Computer Forensics performed or with analyze digital device, whether the device is a media Actors or as a media victim. Digital Forensic Analysis Being divided into two, traditional / dead and alive. Forensic analysis traditionally involves digital data Deposited permanent Operates in Irish, while live forensic analysis involves analysis of data Namely temporary in Random Access Memory or Deposited hearts transport equipment in the Network. Singer proposes journal Forensic analysis of life in the latest operation system windows 10. That study focused IN case several email security browsers Sales Operations manager of Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer Edge. In addition, although many digital forensics type software applications not free, goal on research objectives compares browser security information so it will be more minimize abuse email..

Keywords : Live Forensics, Browser, Email

Digital forensik menjadi salah satu istilah popular saat ini karena banyaknya pelanggaran cyber crime. Teknik Digital forensik dilakukan dengan menganalisis komputer atau perangkat digital, apakah perangkat itu sebagai media pelaku atau sebagai media korban. Analisis digital forensik terbagi menjadi dua, yaitu tradisional/dead dan live. analisis forensik digital tradisional menyangkut data yang disimpan secara permanen di perangkat, sedangkan analisis live forensic yaitu analisis menyangkut data sementara yang disimpan dalam peralatan atau transit di jaringan. jurnal ini mengusulkan analisis forensik live di system operasi terbaru yaitu windows 10. Studi kasus berfokus pada kemanan email beberapa browser secara umum Google Chrome, Mozilla Firefox, dan Microsoft Edge Internet Explorer. Selain itu, meskipun banyak jenis aplikasi software digital forensic yang berbayar, Hasil Eksperimen penelitian ini yaitu membandingkan browser dari segi kemanan informasi sehingga akan lebih meminimalkan penyalahgunaan email.

Kata Kunci : Live Forensics, Browser, Email

1. PENDAHULUAN

Digital forensic merupakan ilmu baru yang berkembang terus-menerus sehingga perlu mendalam belajar tentang ilmu ini. Ilmu digital forensic berubah karena perkembangan system operasi, smartphone, dan tablet (Hausknecht, Foit, & Burić1, 2015) (Rahardjo, 2002). Langkah-langkah digital forensic yang banyak dan rumit ini membutuhkan kemampuan dan software khusus untuk memecahkan suatu permasalahan yang terjadi (Carrier, 2009). Analisis digital forensic 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 system atau data volatile yang umumnya tersimpan pada Random Access Memory (RAM) atau transit pada jaringan (Faiz, Umar, & Yudhana, 2016).

Digital forensic pada intinya adalah dapat 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 (Gianni & Solinas, 2013).

Penelitian yang dilakukan oleh Ellick M. Chan tahun 2011 pada disertasinya bahwa urutan langkah dalam membantu menangani suatu masalah digital forensics yaitu :

1. Preparation : Siapkan peralatan dan alat-alat untuk melakukan tugas-tugas yang diperlukan selama penyelidikan.
2. Collection : Cari, dokumen, dan mengumpulkan atau membuat salinan dari objek fisik yang berisi bukti elektronik.
3. Examination : Membuat bukti elektronik terlihat dan dokumen dari isi sistem. reduksi data dilakukan untuk mengidentifikasi bukti.
4. Analysis : Menganalisis bukti dari tahap Pemeriksaan untuk menentukan fi signicance dan nilai pembuktian.
5. Reporting : Buat catatan pemeriksaan setelah setiap kasus.

Dari penelitian tersebut Ellick M. Chan merujuk pada The U.S. National Institute of Justice (NIJ) (Chan E. M., 2011) (Justice, 2001).

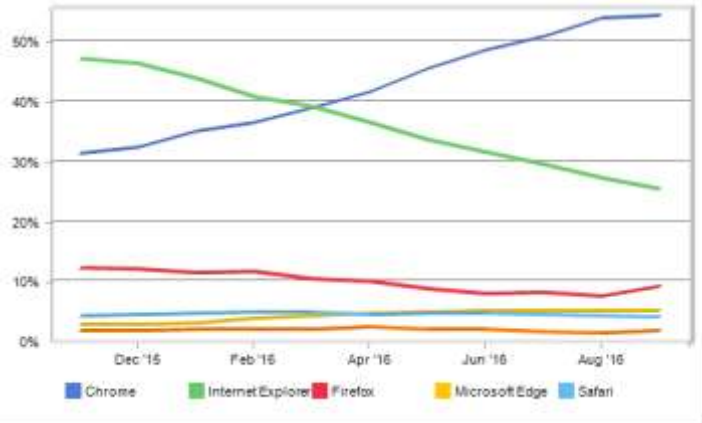
Live forensic dapat dilakukan ketika sistem belum mati atau down, karena hampir kesuluruhan penggunaan system tersimpan pada RAM, pagefile, hibernation file dan crash dump file (Neethu Joseph & Dija S, 2014) (Carrier, 2009). Tujuan pentingnya analisis data pada RAM, yaitu dapat mengetahui letak data tersebut dan isi data tersebut. Semua data pada computer 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 (Chan, 2011) (Ligh, A. Case, & Aron, 2014) (Ligh, Adair, Hartstein, & Richard, 2010).

Sejarah internet (International Networking) yaitu berawal dari penelitian untuk pertahanan pada perang dunia pertama. Internet menjadi sangat penting dalam kehidupan sehari-hari, aplikasi yang digunakan untuk melakukan internet biasa disebut dengan browser. Jenis browser saat ini semakin banyak dan berkembang dengan pesat diantaranya Google Chrome, Mozilla Firefox, Microsoft Edge, Internet Explore, Safari, Opera dan lainnya (Bickford & Giura, 2015) (Jones & Etzkorn, 2016).

Berhubungnya antara system 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 (Rahardjo, 2002).

Microsoft Edge merupakan pramban yang dikembangkan oleh system operasi windows dan dirilis pada tanggal 29 Juli 2015. Pramban ini merupakan pengganti dari Internet Explorer pada Windows 10 dan dikembangkan di bawah nama kode Project Spartan. Pramban ini juga dirancang untuk menjadi lebih ringan dan mendukung integrase dengan layanan Microsoft lainnya (https://id.wikipedia.org/wiki/Microsoft_Edge, n.d.).

Google melancarkan web browser dengan meluncurkan Chrome, sebuah web browser yang memiliki kecepatan, kemudahan penggunaan yang baik. Mozilla Firefox dibuat oleh mozilla corporation, firefox adalah salah satu web browser open source yang dibangun dengan Gecko layout engine. Tak hanya handal firefox juga didukung oleh sejumlah Add-ons yang dapat diinstall terpisah yang memungkinkan pengguna melakukan sesuai dengan kegunaan Add-ons tersebut (Suryani, 2008-2014).



Gambar 1. Grafik penggunaan browser November, 2015 to September, 2016 (http://www.netmarketshare.com/, n.d.).

Grafik di atas menunjukan sejak bulan November tahun 2015 sampai dengan bulan September 2016 penggunaan Google Chrome terus mengalami peningkatan dari 31.4% hingga 54.4%, penggunaan internet explorer terus mengalami penurunan yaitu dari 47.2% menjadi 25.4%, Pengguna Firefox sendiri tidak stabil dari bulan November 2015 hingga Juni 2016 ada penurunan, kemudian naik sebesar 0.14% pada bulan Juli 2016 dan kembali menurun sebesar 0.43% pada bulan Agustus, bulan selanjutnya kembali mengalami kenaikan sebesar 1.5%. Pengguna Microsoft Edge terus mengalami kenaikan walaupun tidak signifikan. Untuk browser Safari juga fruktuatif, sejak November 2015 sampai dengan Maret 2016 mengalami kenaikan, bulan April turun sebesar 0.4%, kemudian naik 0.2% pada bulan Mei, bulan Juni masih stabil pada 4.6% dan kembali mengalami penurunan sampai bulan September hingga 4.0%. Pengguna browser lainnya juga fruktuatif untuk angka tertinggi yaitu 2.4% pada bulan April 2016 dan angka terendah yaitu 1.5% pada bulan Agustus 2016.

Browser sendiri terus mengalami perkembangan mulai dari fitur sampai kecepatan browsing. Fasilitas tabbed browsing, RSS feeds, berbagai macam widget serta tools tambahan sampai template atau tampilan yang bisa kita ganti sesuai keingian kita. Adanya pengembangan fitur - fitur termasuk fitur kemanan karena internet rawan akan kerentanan informasi. Informasi dan internet merupakan suatu keterkaitan, hampir seluruh pertukaran informasi terjadi pada internet termasuk email untuk media berkomunikasi. Email adalah Electronic mail (Surat elektronik), merupakan metode surat menyurat dari menulis, mengirim, menerima dan menyimpan surat melalui sebuah sistem komunikasi elektronik.

Saat ini mulai banyak bermunculan perusahaan-perusahaan yang menerapkan konsep virtual office, dimana perusahaan tersebut secara fisik tidak ada. Sehingga perusahaan yang termasuk kategori ini menggunakan website dan email sebagai media untuk berkomunikasi dengan pelanggannya dan dengan perusahaan-perusahaan lainnya. Disamping kelebihan yang ditawarkan oleh email, terdapat juga kelemahan-kelemahan di dalamnya. Salah satunya adalah isu keamanan email (Arif, 2007).

	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 2. Akun Email Seluruh Dunia dan Prakiraan Pengguna (M), 2015-2019
(http://www.netmarketshare.com/, n.d.)

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 dating.

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 3. Lalu Lintas Email Setiap Hari 2016-2019 (http://www.netmarketshare.com/, n.d.)

Pada 2015, jumlah email yang dikirim dan diterima per total hari selama 205 miliar. Angka ini diperkirakan akan tumbuh tiap tahunnya rata-rata 3% selama empat tahun berikutnya, mencapai lebih dari 246 miliar pada akhir 2019.

Business Email	2015	2016	2017	2018	2019
Average Number of Emails Sent/Received per	122	123	124	125	126
Average Number of Emails Received	88	90	92	94	96
Average Number of Legitimate Emails	*76*	*76*	*76*	*76*	*77*
Average Number of Spam Emails	*12*	*14*	*16*	*18*	*19*
Average Number of Emails Sent	34	33	32	31	30

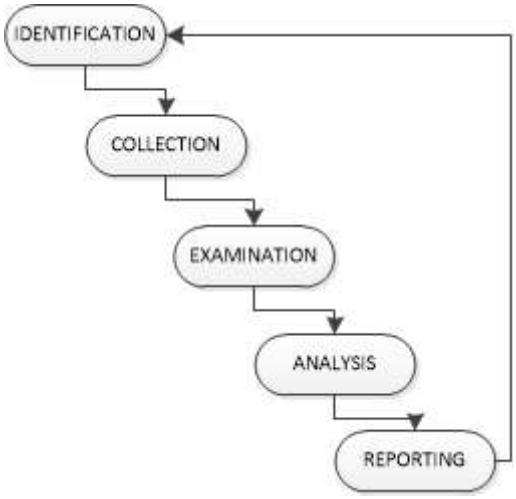
Gambar 4. Lalu Lintas Email Bisnis Terkirim / Diterima Per User / Hari, 2015-2019
(http://www.netmarketshare.com/, n.d.)

Pada tahun 2015, jumlah email bisnis dikirim dan diterima per pengguna per total hari 122 email per hari. Angka ini terus menunjukkan pertumbuhan dan diharapkan. Rata-rata 126 pesan yang dikirim dan diterima per pengguna bisnis pada akhir 2019. Dari Gambar 2, 3, dan 4 maka setiap tahunnya akan mengalami peningkatan penggunaan email di seluruh dunia, sehingga diperlukan pula browser yang dapat mengamankan informasi pribadi, kecepatan mengirim maupun menerima dan fitur yang lebih baik.

Saat ini email merupakan hal yang wajib bagi para pengguna smartphone, komputer, tablet dan yang lainnya, email berguna untuk memudahkan manusia berkomunikasi. e-Mail menyediakan komunikasi dengan biaya yang murah, mudah, dan dapat dipercaya di seluruh dunia. Pesan e-Mail 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 (Arif, 2007).

2. METODE PENELITIAN

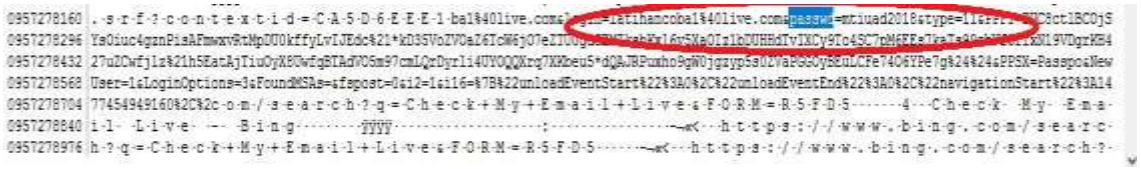
Berdasarkan penelitian yang dilakukan oleh Ellick M. Chan maka peneliti akan menggunakan metodologi penelitian The U.S. National Institute of Justice (NIJ) yang digambarkan dengan alur sebagai berikut :



Gambar 5. Metode Tahapan Digital Forensics

3. HASIL DAN PEMBAHASAN

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 logi pada Mozilla Firefox , latihancoba1@live.com login pada Microsoft Edge.



Gambar 6. Microsoft Edge type public terlihat username dan password

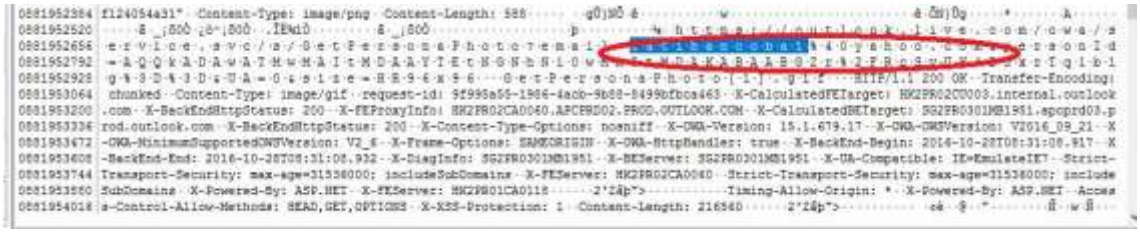
Dari Gambar 6 menunjukkan bahwa Microsoft Edge dengan type public terlihat dengan jelas username dan passwordnya yaitu dengan username latihancoba1@live.com dan password mtiuad2016.

Gambar 7. Google Chrome type public terlihat isi email

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

Gambar 8. Google Chrome type public terlihat subject email

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



Gambar 9. Microsoft Edge type private terlihat kontak

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

Gambar 10. Mozilla Firefox type private terlihat username

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

Berdasarkan hasil eksperimen yang telah dilakukan maka didapatkan hasil perbandingan sesuai dengan Tabel 1.

Tabel 1. Hasil Perbandingan Browser untuk email

Browser	Type	Username	Recepient	Body	Subject	Password
Microsoft Edge	Public	Yes	No	No	No	Yes
Mozilla Firefox	Public	Yes	No	No	No	Yes
Google Chrome	Public	Yes	Yes	Yes	Yes	No
Microsoft Edge	Private	Yes	Yes	No	No	No
Mozilla Firefox	Private	Yes	No	No	No	No
Google Chrome	Private	No	No	No	No	No

Dari tabel 1 dapat dilihat bahwa untuk type public dengan browser Microsoft Edge, Mozilla Firefox dan Google Chrome username masih dapat terlihat sedangkan untuk penerima atau recipient, body dan subject email hanya Google Chrome yang hanya dapat dilihat sedangkan untuk password sebaliknya yaitu hanya Google Chrome yang hanya tidak terlihat.

Untuk type private username hanya dapat terlihat pada Microsoft Edge dan Mozilla Firefox sedangkan Google Chrome tidak, untuk recipient hanya terlihat pada browser Microsoft Edge, browser yang lain tidak terlihat. Untuk body, subject dan password semua browser dengan type private tidak terlihat.

4. KESIMPULAN

Browser merupakan salah satu aplikasi yang berguna untuk menerjemahkan HTML menjadi Bahasa yang dapat dipahami oleh user. Keamanan pada browser merupakan suatu tantangan tersendiri untuk mengembangkan fitur kemanan dan kemudahan dalam menggunakan browser. Microsoft Edge merupakan browser default dari Windows 10 dengan berbagai fitur yang lebih baik dari Internet Explorer namun ternyata untuk segi keamanan lebih lemah jika dibandingkan dengan browser Mozilla Firefox, sedangkan Google Chrome lebih kuat pada passwordnya.

DAFTAR PUSTAKA

Arif, M. R. (2007). e-Mail Security. *Seminar Nasional Teknologi 2007*.

Bickford, J., & Giura, P. (2015). Safe Internet Browsing using a Transparent Virtual Browser. *IEEE*, pp. 423-432.

Carrier, B. D. (2009). Digital Forensics Works. *IEEE*, pp. 26-29.

Chan, E. M. (2011). *https://www.ideals.illinois.edu.* Retrieved from https://www.ideals.illinois.edu/bitstream/handle/21, diakses 25 Oktober 2016

Faiz, M. N., Umar, R., & Yudhana, A. (2016). ANALISIS KINERJA METODE LIVE FORENSICS UNTUK INVESTIGASI . *Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM) Prosiding Konferensi Nasional Ke- 4* , pp. 207-211.

Gianni, F., & Solinas, F. (2013). Live Digital Forensics: Windows XP vs Windows 7. *IEEE*, pp. 1-6.

Hausknecht, K., Foit, D., & Burić1, J. (2015). RAM data significance in Digital Forensics. *IEEE Conference Publications*, pp. 1372 - 1375.

http://www.netmarketshare.com/. (n.d.). diakses 24 Oktober 2016

https://id.wikipedia.org/wiki/Microsoft_Edge. (n.d.). Retrieved from https://id.wikipedia.org/wiki/Microsoft_Edge, diakses 24 Oktober 2016

Jones, J., & Etzkorn, L. (2016). Analysis of Digital Forensics Live System Acquisition Methods to Achieve Optimal Evidence Preservation. *IEEE*, pp. 1-6.

Ligh, M. H., A. Case, J. L., & Aron, A. (2014). *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory.* Indianapolis: simultaneously.

Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2010). *Malware Analyst's Cookbook.* Indianapolis: Wiley Publishing,.

Neethu Joseph, S. S., & Dija S, T. K. (2014). Volatile Internet Evidence Extraction from Windows. *IEEE*, pp. 1-5.

Rahardjo, B. (2002). *Keamanan Sistem Informasi Berbasis Internet.* Jakarta: PT INDOCISC - Jakarta.

Suryani, L. (2008-2014). *http://ilmuti.org.* Retrieved from http://ilmuti.org/wp-content/uploads/2014/03/Lely-Suryani-Mengenal-Macam-Macam-Web-Browser1.pdf , diakses 26 Oktober 2016