STUDI BANDING EMAIL FORENSIC TOOLS

Tulus Hadianto[1], Widi Prasetyo[2] , Rizal Broer Bahaweres[3]

[1,2,3]Jurusan Teknik Elektro, Fakultas Teknik Universitas Mercu Buana, Jakarta
[3]Program Studi Teknik Informatika, Fakultas Sains dan Teknologi
Universitas Islam Negeri (UIN) Syarif Hidayatullah Jakarta
Email: widi.prasetyo@outlook.com ; tulushadianto@gmail.com ; rizalbroer@ieee.org

ABSTRACT

Over the last few decades, email has become a carrier source for transporting spam and malicious content. The Email Network is also a major source of criminal activity on the Internet. Computer Forensics is a systematic process for storing and analyzing email stored on a computer for the purpose of proof in legal proceedings and other civil matters. Email analysis is challenging because it is not only used in various fields that can be done by hackers or malicious users, but also the flexibility of composing, editing, deleting email using offline (eg, MS Outlook) or online email (eg Webmail) applications. To anticipate this, an approach is taken using email forensic tools to understand the extent to which these tools will be useful for detecting and performing appropriate forensic analysis. In this paper, we conducted a comparative study of a set of common features to compare and compare five popular opensource tools forensic email. The study found that all forensic email tools are not similar, offering all types of facilities. Combining these tools allows analysis to get detailed information in the field of forensic email.

Keywords: *Forensic Email, Header and Content Analysis, Data Recovery, Search Option, Visualization*

ABSTRAK

Selama beberapa dekade terakhir, email telah menjadi sumber pembawa untuk mengangkut spam dan malicious content. Jaringan Email juga merupakan sumber utama berbagai kegiatan kriminal di Internet. Computer Forensics adalah proses yang sistematis untuk menyimpan dan menganalisis email yang tersimpan di dalam komputer dengan tujuan sebagai bukti dalam proses hukum dan masalah perdata lainnya. Analisis email menantang karena tidak hanya dipergunakan dalam berbagai bidang yang bisa dilakukan oleh hacker atau malicious users, tapi juga fleksibilitas composing, mengedit, menghapus email menggunakan offline (misalnya, MS Outlook) atau email online (misal : Email Web) aplikasi. Untuk mengantisipasi hal tersebut maka diambil sebuah pendekatan dengan menggunakan email forensic tools untuk memahami sejauh mana tools ini akan berguna untuk mendeteksi dan melakukan analisis forensik yang sesuai. Di makalah ini, kami melakukan studi banding dari sekumpulan fitur umum untuk membandingkan dan membandingkan lima opensource tools yang populer email forensic. Studi ini menemukan bahwa semua email forensic tools tidak serupa, menawarkan semua jenis fasilitas. Dengan menggabungkan tools ini memungkinkan analisa mendapatkan informasi rinci di bidang email forensic.

Kata kunci : Email Forensic, Header and Content Analysis, Data Recovery, Search Option, Visualization

I. PENDAHULUAN

Email merupakan metode umum untuk berkomunikasi antara dua belah pihak. Hal tersebut merupakan file transfer antara dua server pada nomor port yang spesifik[1]. Sebuah email biasanya ditulis pada sebuah aplikasi yang ada pada sisi client(Web Client, MS Outlook, Lotus notes) dengan identitas pengirim, disimpan dalam bentuk file, lalu dikirimkan ke alamat tujuan melalui satu atau beberapa server. Meskipun komunikasi melalui Email telah dirancang agar segalanya menjadi lebih mudah, efisien, dan powerful[2], penulisan Email dan komunikasinya telah menjadi fokus dari penyusup selama beberapa puluh tahun. Kami menemukan bahwa sangat biasa Email menjadi sumber transportasi untuk mengantarkan isi pesan yang mengganggu, jahat, phishing, dan spam.

Saat ini, banyak teknologi yang telah dikembangkan untuk memeriksa dan melindungi email yang termasuk didalamnya deteksi spam, deteksi email spam, penyaringan isi dan lampiran email(anti-virus). Salah satu aspek kunci untuk merancang dan mengembangkan teknologi tersebut adalah melakukan investigasi forensik pada email sample agar dengan benar mengenali informasi penting seperti nama atau identitas penerima, jalur yang digunakan antara pengirim dan penerima untuk mengantarkan email, aplikasi pada sisi client yang digunakan untuk menulis email, timestamp kapan email tersebut di-generate, message ID unik, dll. Pada literatur, pemeriksaan dan pengungkapan informasi kunci dari sebuah email disebut sebagai Email Forensics[3][4]. Contoh umum atas penggunaan forensik adalah untuk memahami fakta kunci dan mengandalkan hal tersebut untuk prosedur hukum.

Dua puluh tahun belakangan ini, banyak email forensic tools telah dikembangkan. Menurut

Garfinkel[5], kebanyakan dari tools tersebut ([6]-[10]) berbeda, dan tidak berdasarkan pada pekerjaan sebelumnya. Bahkan, kebanyakan tools dikembangkan pada permasalahan tersendiri. Lebih jauh lagi, kebanyakan forensic tools tidak dimaksudkan untuk menyelesaikan permasalahan cyber dan computer crime secara spesifik. Mereka dimaksudkan untuk menemukan dan memulihkan informasi. Jika demikian, maka akan muncul pertanyaan diantara stakeholder: sampai dimana tools yang ada cocok untuk melakukan investigasi digital forensic? Paper ini bermaksud untuk menjawab pertanyaan tersebut dengan membandingkan dan membedakan beberapa email forensic tools yang populer. Secara khusus, fokus kami ada pada analisa email header yang ditawarkan oleh masing-masing tools. Kami memeriksa kemampuan dari beberapa email forensic tools yang populer yaitu : MainXaminer[6], Add4Mail[7], Digital Forensic Framework[8], eMailTrackerPro[9], dan Paraben Email Examiner[10]. Pekerjaan kami merupakan penambahan dari penelitian sebelumnya yang berusaha untuk memahami kemampuan dari tipe forensic tools lainnya seperti network forensics[4] dan disk/memory forensic tools[11].

Paper ini ditulis sebagai berikut: bagian 2 bicara tentang overview dari elemen email header dan prosedur email forensic secara umum. Bagian 3 bicara tentang analisa beberapa open source tools berdasarkan atributnya. Akhirnya pada bagian 4 merupakan kesimpulan dari paper ini.

II. LATAR BELAKANG

A. Apa isi dari Email Header?

Sebuah email memiliki header dan body. Header memiliki banyak informasi penting seperti alamat IP pengirim, mail user agent, transit server, message id field, dan signatures field. Berikut adalah contoh dari email header pada gambar 1.

```
Received: (qmail 20564 invoked from network); 5 Jan 2006 16:11:57 −0000
From: foo<foo@foo.com>
To: bar@bar.com
Subject: Test
User-Agent: KMail/1.9
MIME-Version: 1.0
Content-Disposition: inline
Date: Thu, 5 Jan 2006 16:41:30 +0100
Content-Type: text/plain; charset = “iso-8859-1”
X-Originating-IP: [216.119.20.3]
Message-Id: <200601051641.31830.foo@foo.com>
X-HE-Spam-Score: 0.0
X-HE-Virus-Scanned: yes
Status: OR
Content-Length: 124
Lines: 26
```

Gambar 1. Screenshot Email Header

Received field menunjukkan tanggal dan waktu kapan email tersebut diterima server. From and To menunjukkan pengirim dan penerima. user-agent field menunjukkan aplikasi pada sisi client yang digunakan untuk menulis email. Versi dari Multipurpose Internet Mail Extensions (MIME) menunjukkan 1.0. Content Disposition header menunjukkan gaya penampilan dari email tersebut. Pada contoh di atas, inline content-disposition berarti bahwa pesan email seharusnya secara otomatis ditampilkan (sebagai text yang juga diindikasikan pada content-type) dan tidak ada lampiran. X-Originating-IP mengindikasikan sumber alamat IP dimana email tersebut di-generate. Date adalah waktu ketika email di-generate. Message id adalah sebuah ID yang di-generate secara otomatis dimana informasi dari timestamp itu ada dan bersamaan dengan informasi akun pengirim. X-HE-Spam-Level berisi nilai spam yang dihitung pada sisi client (untuk mencegah spammming). Status: OR mengindikasikan bahwa pesan email di-download tetapi tidak dihapus (lihat http://www.faqs.org/rfcs/rfc2076.html untuk lebih jelas; Pada contoh, R berarti pesan dibaca atau di-download, dan O berarti pesan tersebut sudah lama namun tidak dihapus). Content-Length menunjukkan panjang dari pesan email (dalam bytes).

Analisa email pada cyber forensic diharuskan untuk mengumpulkan bukti yang kredible untuk mengantarkan kriminal kepada hukum, khususnya pada bagian analisa header[12]. Analisa header yang mendetail dapat digunakan untuk memetakan jaringan yang dilewati oleh pesan email. Jika ada beberapa field informasi yang diterima, maka asal email tersebut dapat diurutkan dari bawah ke atas, dimana alamat IP yang berada dibawah merupakan original IP pengirim dan alamat IP yang berada diatas merupakan alamat IP Penerima.

B. Langkah-Langkah Analisis Email Forensics

Investigasi forensik dari sebuah email dapat memeriksa kedua email header dan body. Namun, paper ini hanya akan melihat ke arah pemeriksaan header. Menurut marwan[12] sebuah investigasi harus memiliki sebagai berikut:

- Pemeriksaan alamat email pengirim
- Pemeriksaan protokol pesan email (HTTP, SMTP)
- Pemeriksaan Message ID
- Pemeriksaan alamat IP pengirim

Beberapa aspek yang mengatur langkah forensik memiliki properti sebagai berikut:

1) Format penyimpanan email: format penyimpanan pada sisi server mungkin akan memiliki maildir (setiap email disimpan secara terpisah dalam sebuah file, untuk setiap user), format mbox (semua file email dalam bentuk sebuah file text). Pada sisi server email disimpan dalam basis data SQL server. Membaca tipe format yang berbeda-beda dapat dilakukan untuk analisa forensik dengan menggunakan notepad editor dan menggunakan regular expression-based search[1]. Pada sisi client,

sebuah email disimpan sebagai format mbox (Thunderbird)[1]. Sisi client juga mungkin menyimpan email dalam bentuk .PST(MSOutlook), dan NSF(LotusNotes) files.
2) Ketersediaan backup copy dari email: Ketika sedang memeriksa dari sisi server, semua salinan dari email akan dikirimkan kepada client. Oleh sebab itu diperlukan penyitaan komputer client. Sedangkan untuk webmail, salinan email akan tetap ada pada sisi server[1].
3) Protokol pengiriman email: Email dapat diinisiasikan dan dikirimkan melalui SMTP atau HTTP[12] tergantung dari aplikasi server email.

III. KRITERIA FORENSIC TOOLS

Kami membandingkan email forensic tools berdasarkan pada atribut yang dibutuhkan oleh forensic tools sebagaimana telah disebutkan pada artikel Garfinkel[2] yang berfokus pada permasalahan bantuan investigasi forensik yang tidak dapat digeneralisasikan pada banyak kasus. Bersamaan dengan hal tersebut, kriteria yang diharapkan haruslah relevan dengan kemampuan reverse engineering, peningkatan pengolahan data, dengan mempertimbangkan adanya perubahan teknologi untuk penyimpanan, transportasi data, dan environment antara pemrosesan devices and penyimpanan inputs.

Kami mengidentifikasi sembilan kriteria yang mungkin berguna dan dimiliki oleh forensic tools sebagai berikut:
1) Kebutuhan input file pada hard disk,
2) Search option
3) Informasi yang diperoleh atau disediakan oleh forensic tools
4) Kemampuan recovery
5) email file format supported
6) visualization support
7) operating system (OS) supported
8) extended device supported
9) and export format supported.

Kami mencari literatur dan halaman web untuk mengidentifikasi email forensic tools yang tersedia di dunia nyata[4] [12]-[14]. Kami memilih lima open source email tools yang populer dan banyak digunakan.

Kriteria Tools	Email Forensic Tools				
	Mail Xaminer	Add4 Mail	Digital Forensic Framework	eMail TrackerPro	Paraben E-Mail Examiner
Input file					
In disk required	√	√	√	√	√
Directly to Webmail IMAP services (Gmail, Yahoo! Mail, AOL Mail, FastMail, GMX Mail, Outlook.com, Outlook 356)		√			
Search option					
Plain text-based search	√	√	√		
Exported PDF-based search		√	√		
Filter the emails based on text, time, date, keywords, logical operators, and regular expressions		√	√		
Search mail by date, header content, and by message body content		√	√		
Search based on dictionaries			√		
Search based on email content, tags, and time-line			√		
Performs comprehensive analysis features, bookmarking, advanced boolean searching, and searching within attachments					√
Search based on unicode					√
Information provided					
Shows the message, date and time details	√	√	√		
Perform like virtual machine disk reconstruction			√		
IP Address with Geographic Location				√	
Display any port open at IP address				√	
Examine email headers and bodies message					√
Recovery capability					
Recover corrupted email jenis :					
NSF	√		√		√
EDB	√		√		√

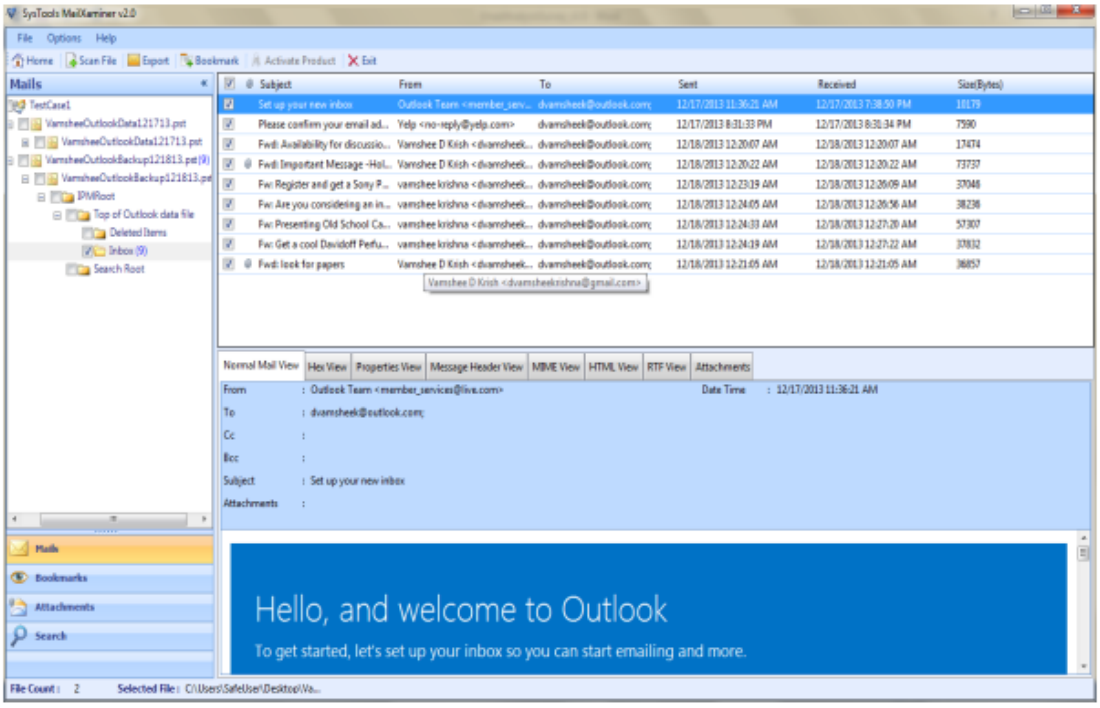
	EML	√		√		√
	PST	√		√		√
	OST	√		√		√
	OLM	√		√		√
	IMM	√		√		√
	TBB	√		√		√
	MBX	√		√		√
	MBOX	√		√		√
Proses Deleted email jenis :						
	NSF	√	√	√		√
	EDB	√	√	√		√
	EML	√	√	√		√
	PST	√	√	√		√
	OST	√	√	√		√
	OLM	√	√	√		√
	IMM	√	√	√		√
	TBB	√	√	√		√
	MBX	√	√	√		√
	MBOX	√	√	√		√
Filter duplicate emails			√			
Recover emails from the trash folder			√			
Restore unpurged emails			√			
Not Available					√	
Visualization support						
Available in : Hexa-decimal content inspection, Normal inspection, Property inspection, Email Header, MIME inspection, Email Hop View, viewing in HTML and RTF format		√				
Like Outlook Message Display					√	
Not Available			√	√		√
Email file format supported						
Gmail		√	√	√	√	√
Yahoo		√	√	√	√	√
Hotmail		√	√	√	√	√
IMAP		√	√	√	√	√
Mozilla Thunderbird		√	√	√	√	√
Lotus Notes		√	√	√	√	√
Outlook		√	√	√	√	√
Exchange		√	√	√	√	√
Mac Outlook		√	√	√	√	√
(OS) supported						
Windows 32 bit		√	√	√	√	√
Windows 64 bit		√	√		√	√
Linux			√	√		
Macintosh			√			
Export format supported						
Provides export options in plain text file, EML, PST, TIFF, PDF, MSG and HTML		√	√	√		√
Provide export list IP address, DNS in excell or HTML					√	
Extended device supported plug-ins devices						
Supported			√	√		
Not Supported		√			√	√

Kami akan memberikan nilai performa, dimana setiap kemampuan diberi nilai "1" (satu) dan akan terlihat seperti dalam tabel berikut ini :

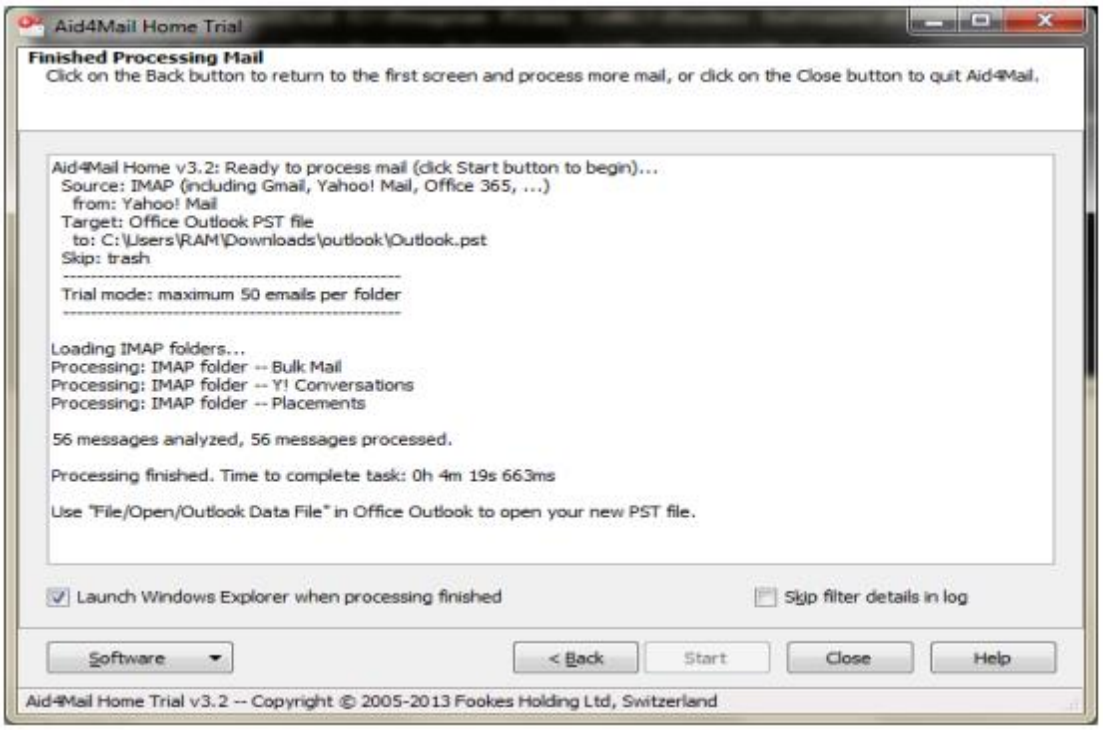
Kriteria Tools	Email Forensic Tools				
	MailXaminer	Add4Mail	Digital Forensic Framework	eMail TrackerPro	Paraben E-Mail Examiner
Input file					
In disk required	1	1	1	1	1
Directly to Webmail IMAP services (Gmail, Yahoo! Mail, AOL Mail, FastMail, GMX Mail, Outlook.com, Outlook 356)		1			
Search option					
Plain text-based search	1	1	1		
Exported PDF-based search		1	1		
Filter the emails based on text, time, date, keywords, logical operators, and regular expressions		1	1		
Search mail by date, header content, and by message body content		1	1		
Search based on dictionaries			1		
Search based on email content, tags, and time-line			1		
Performs comprehensive analysis features, bookmarking, advanced boolean searching, and searching within attachments					1
Search based on unicode					1
Information provided					
Shows the message, date and time details	1	1	1		
Perform like virtual machine disk reconstruction			1		
IP Address with Geographic Location				**1**	
Display any port open at IP address				1	
Examine email headers and bodies message					1
Recovery capability					
Recover corrupted email jenis : , EML, PST, OST, OLM, IMM, TBB, MBX and MBOX					
NSF	1		1		1

EDB	1		1	1
EML	1		1	1
PST	1		1	1
OST	1		1	1
OLM	1		1	1
IMM	1		1	1
TBB	1		1	1
MBX	1		1	1
MBOX	1		1	1
Proses Deleted email jenis : NSF, EDB,				
NSF	1	1	1	1
EDB	1	1	1	1
EML	1	1	1	1
PST	1	1	1	1
OST	1	1	1	1
OLM	1	1	1	1
IMM	1	1	1	1
TBB	1	1	1	1
MBX	1	1	1	1
MBOX	1	1	1	1
Filter duplicate emails		1		
Recover emails from the trash folder		1		
Restore unpurged emails		1		
Not Available				√

Kriteria Tools	Email Forensic Tools				
	MailXaminer	Add4Mail	Digital Forensic Framework	eMail TrackerPro	Paraben E-Mail Examiner
Visualization support					
Available in : Hexa-decimal content inspection, Normal inspection, Property inspection, Email Header, MIME inspection, Email Hop View, viewing in Like Outlook Message Display	√			1	
Not Available		√	√		√
Email file format supported					
Gmail	1	1	1	1	1
Yahoo	1	1	1	1	1
Hotmail	1	1	1	1	1
IMAP	1	1	1	1	1
Mozilla Thunderbird	1	1	1	1	1
Lotus Notes	1	1	1	1	1
Outlook	1	1	1	1	1
Exchange	1	1	1	1	1
Mac Outlook	1	1	1	1	1
(OS) supported					
Windows 32 bit	1	1	1	1	1
Windows 64 bit	1	1		1	1
Linux		1	1		
Macintosh		1			
Export format supported					
Provides export options in plain text file, EML, PST, TIFF, PDF, MSG and HTML	1	1	1		1
Provide export list IP address, DNS in excell or HTML				1	
Extended device supported plug-ins devices					
Supported		1	1		
Not Supported	√			√	√
Nilai Performa	**35**	**35**	**42**	**16**	**36**



Gambar 2. Snapshot analisa email dengan MailXaminer untuk outlook mail



Gambar 3. Snapshot analisa email dengan Add4Mail

IV. KESIMPULAN

Penelitian ini merupakan analisa perbandingan lima open source email forensic tools yaitu MailXaminer, Aid4Mail, Digital Forensic Framework, eMailTrackerPro, and Paraben Email Examiner. Kami membandingkan forensic tools tersebut dengan menggunakan sembilan kriteria: input file, search option, information provided, recovery capability, format supported, visualization format supported, operating system supported, export format, and extended device support.

Hasil analisa kami dengan mengambil **nilai performa terbesar yaitu 42 (Empat Puluh Dua) adalah email forensic tool dengan nama aplikasi Digital Forensic Framework.**

Hasil analisa kami menunjukkan bahwa dari antara kelima forensic tools, Add4Mail dapat menganalisa email yang disimpan di hard disk(offline analysis) maupun email yang disimpan di server(online analysis).

Pada bagian search option, Add4Mail memiliki jumlah tertinggi untuk kemampuannya dalam mengumpulkan informasi dibandingkan tools forensic lainnya. Diantara semua forensic tools, informasi yang disediakan oleh Paraben Email Examiner tidak hanya meliputi email header dan body, tetapi juga termasuk informasi isi file lampiran.

Kemampuan recovery email oleh Add4Mail dan Paraben E-mail Examiner terlihat lebih baik dibandingkan ketiga forensic tools lainnya. Hal tersebut dikarenakan mereka mampu menyelamatkan file email dari folder delete.

Email format, Paraben E-mail Examiner mendukung kebanyakan dari email format yang telah diketahui dan 750 MIME tipe isi email. Namun, untuk dukungan visualisasi, MailXaminer menyediaakan berbagai macam pilihan untuk end users. Kebanyakan forensic tools , menggunakan windows sebagai sistem operasinya, sementara hanya beberapa yang menggunakan Linux.

Digital Forensic Framework memiliki output yang kaya akan tipe format file. Akhirnya, sangat sedikit forensic tools (Add4Mail, Digital Forensic Framework) yang mendukung alat tambahan seperti USB memory stick. Semakin banyak kriteria yang dimiliki oleh forensic tools, semakin baik pula kemampuannya untuk menampilkan berbagai tipe aktifitas forensik dan prosedur hukum.

Penelitian kami selanjutnya meliputi pengukuran performa runtime (CPU, memory) dengan menggunakan email benchmark. Kami berencana untuk memeriksa permasalahan kompabilitas berdasarkan kriteria yang kami usulkan yang mungkin muncul ketika menggunakan berbagai forensic tools untuk menginvestigasi sebuah email yang sama. Pembelajaran selanjutnya meliputi bagaimana email forensic tools dapat diaplikasikan bersamaan dengan complementary network and memory forensic tools.

V. DAFTAR PUSTAKA

[1] Conan Albrecht, Email Analysis. http://www.gsaig.gov/assets/File/other-documents/Forensics-EmailAnalysis.pptx.pdf

[2] McAfee SaaS Email Protection. http://www.mcafee.com/us/resources/solution-briefs/sb-saas-email-protection-solution-guide.pdf

[3] Banday, M. (2011) Analyzing Email Headers for Forensic Investigation. Journal of Digital Forensics, Security, and Law, 6, 50-64.

[4] Meghanathan, N., Allam, S.R. and Moore, L.A. (2009) Tools and Techniques for Network Forensics. International Journal of Network Security and its Applications,1,14-25. http://airccse.org/journal/nsa/0409s2.pdf

[5] Garfinkel, S.L. (2010) Digital Forensics Research: The Next 10 Years. Digital Investigation, 7, S64-S73. http://dx.doi.org/10.1016/j.diin.2010.05.009

[6] MailXaminer. http://www.mailxaminer.com/

[7] Aid4Mail Forensic. http://www.aid4mail.com/

[8] Digital Forensics Framework. http://www.digital-forensic.org/

[9] EMailTrackerPro. http://www.emailtrackerpro.com/

[10] Paraben (Network) E-mail Examiner. http://www.paraben.com/email-examiner.html

[11] Garfinkel, S. (2006) Forensic Feature Extraction and Cross-Drive Analysis. Digital Investigation, 3, 71-81.

[12] Marwan A.Z. (2004) Tracing E-mail Headers. Proceedings of Australian Computer, Network & Information Forensics Conference, November 2004, School of Computer and Information Science, Edith Cowan University Western Australia, 16-30.

[13] Free Computer Forensic Tool. https://forensiccontrol.com/resources/free-software/

[14] Digital Intelligence Forensic Software. http://www.digitalintelligence.com/forensicsoftware.php