BAB 2

Tinjauan Pustaka

2.1 Digital Forensik

Kata “forensik” memiliki arti menyajikan ke pengadilan, sehingga istilah forensik dimaksudkan sebagai suatu proses ilmiah (didasari oleh ilmu pengetahuan) dalam mengumpulkan, menganalisis, dan menghadirkan berbagai bukti dalam sidang pengadilan dikarenakan suatu kasus hukum (Sulianta, 2016). Komputer/digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (*pro justice*), yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi atau *computer crime* secara ilmiah (*scientific*) hingga bisa mendapat bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut (Al-Azhar, 2012).

Istilah forensik dapat didefinisikan sebagai penerapan ilmu pengetahuan untuk masalah hukum. Sedangkan definisi dari digital forensik yang paling diterima berasal dari definisi komputer forensik. Definisi komputer forensik adalah pengumpulan, penyimpanan, analisis dan penyajian bukti elektronik untuk digunakan dalam masalah hukum dengan menggunakan proses, alat, dan praktik forensik yang masuk akal dan diterima secara hukum. Secara khusus, digital forensik adalah penerapan teknologi komputer untuk masalah hukum yang buktinya mencakup barang-barang yang dibuat oleh orang-orang dan barang-barang yang dibuat oleh teknologi sebagai hasil interaksi dengan seseorang (Daniel & Daniel, 2011).

Terdapat beberapa klasifikasi dari spesialisasi digital forensik yang cakupannya cukup luas berdasarkan pada bentuk fisik maupun logis dari barang bukti yang diperiksa/dianalisis. Klasifikasinya adalah sebagai berikut (Al-Azhar, 2012):

- *Computer Forensic*

  Forensik ini berkaitan dengan pemeriksaan dan analisis barang bukti elektronik berupa komputer pribadi (*personal computer* atau PC), *laptop/notebook*, *netbook*, dan *tablet*.
- *Mobile Forensic*

  Forensik ini berkaitan dengan jenis barang bukti elektronik yang berupa *handphone* dan *smartphone*.
- *Audio Forensic*

  Forensik ini berkaitan dengan rekaman suara pelaku kejahatan.
- *Video Forensic*

Forensik ini berkaitan dengan barang bukti berupa rekaman video, yang biasanya berasal dari kamera CCTV (*closed circuit tv*).

- *Image Forensic*

  Forensik ini berkaitan dengan jenis barang bukti digital yang berupa *file-file* gambar digital yang sering diperiksa dan dianalisis untuk mengetahui peralatan kamera digital yang digunakan untuk mengambil gambar tersebut, termasuk waktu pengambilannya.

- *Cyber Forensic*

  Forensik ini berkaitan dengan pemeriksaan dan analisis kasus-kasus yang berhubungan dengan internet atau jaringan komputer seperti LAN (*Local Area Network*). Analisis terhadap email termasuk di dalam *cyber forensic*.

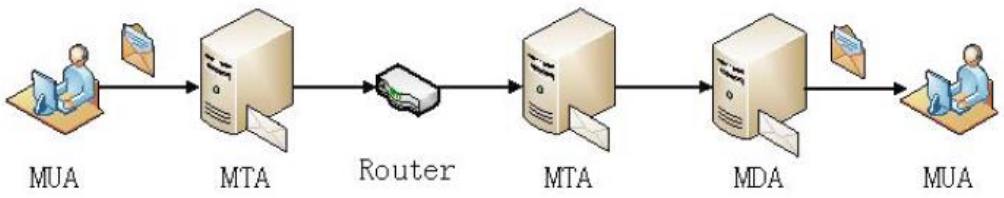
2.2 Bukti Digital

Bukti digital didefinisikan sebagai sekumpulan data yang disimpan atau dikirimkan menggunakan komputer yang mendukung atau menyangkal teori tentang bagaimana suatu pelanggaran terjadi (Casey, 2011). Pengertian lainnya, bukti digital adalah informasi dan data yang berkaitan dengan suatu kasus komputer forensik (Sulianta, 2016).

Pada buku Digital Forensic: Panduan Praktis Investigasi Komputer, barang bukti digital forensik diklasifikasikan menjadi dua, yaitu: barang bukti elektronik dan barang bukti digital. Barang bukti elektronik ini bersifat fisik dan dapat dikenali secara visual, sehingga investigator dan analis forensik harus sudah memahami serta mengenali masing-masing barang bukti elektronik ini ketika sedang melakukan proses pencarian (*searching*) barang bukti di TKP. Barang bukti elektronik ini contohnya: PC, *handphone*, *hard disk*, *router*, kamera digital, dan lain-lain. Sedangkan barang bukti digital adalah barang bukti yang bersifat digital yang diekstrak atau di-*recover* dari barang bukti elektronik. Barang bukti ini dalam Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dikenal dengan istilah "informasi elektronik" dan "dokumen elektronik". Jenis barang bukti ini yang harus dicari oleh analis forensik untuk kemudian dianalisis secara teliti keterkaitan masing-masing file dalam rangka mengungkap kasus kejahatan yang berkaitan dengan barang bukti elektronik. Contoh barang bukti digital: *logical file*, *deleted file*, *log file*, *video file*, *image file*, *email*, dan lain sebagainya (Al-Azhar, 2012).

2.3 Email

Email adalah surat berbasis elektronik yang menggunakan sistem jaringan online untuk mengirimkannya atau menerimanya (Al-Azhar, 2012). Penggunaan email saat ini memainkan peranan penting dalam kehidupan kebanyakan orang dan telah menjadi metode komunikasi utama di antara entitas bisnis (Chung & Ho, 2007). Email menjadi bagian yang penting karena akun email diperlukan untuk mendaftar ke situs jejaring sosial, *instant messaging*, dan layanan lain yang tersedia di internet (The Radicati Group, 2018).



Gambar 2.1 Proses pengiriman email

Proses pengiriman sebuah email diilustrasikan pada Gambar 2.1, yaitu ketika email yang dibuat oleh klien atau disebut MUA (*Mail User Agent*) dikirimkan, email tersebut dialihkan dari satu server ke server lainnya sampai ke server email penerima. Lebih tepatnya, email tersebut dikirim ke server yang bertugas untuk mengirim email atau MTA (*Mail Transport Agent*) ke MTA penerima. MTA penerima kemudian mengirimkan email ke server kotak masuk atau MDA (*Mail Delivery Agent*) yang menyimpan email saat menunggu penerima untuk menerimanya (Guo, Jin, & Qian, 2013).

Suatu email terdiri bagian *header* dan *body*. Bagian *header* memuat banyak informasi penting seperti alamat IP pengirim, *mail user agents*, *server* yang digunakan selama perjalanan dari pengirim ke penerima, *message id*, dan *signatures* (Devendran et al., 2015).

Tabel 2.1 menunjukkan contoh *header* dari sebuah email yang dikirimkan oleh tariq@tariq.com yang berpura-pura menjadi alice@alice.com dan dikirim ke bob@bob.com. Dalam email tersebut, alamat pengirim, tanggal pengiriman, alamat balasan dan beberapa *field* lainnya telah dipalsukan. Identitas seperti nama domain, alamat IP, dan lainnya yang dapat mengungkapkan server yang digunakan dalam proses pengiriman email telah diedit dengan tepat. Kumpulan *header* ini digunakan untuk menunjukkan informasi yang terkandung di dalamnya.

Tabel 2.1 Contoh *header* email

No.	Header	Value
1.	*X-Apparently-To:*	bob@bob.com via a4.b4.c4.d4; Tue, 30 Nov 2010 07:36:34 -0800
2.	*Return-Path:*	< alice@alice.com >
3.	*Received-SPF:*	none (mta1294.mail.mud.bob.com: domain of alice@alice.com does not designate permitted sender hosts)
4.	*X-Spam-Ratio:*	3.2
5.	*X-Originating-IP*	[a2.b2.c2.d2]
6.	*X-Sieve:*	CMU Sieve 2.3
7.	*X-Spam-Charsets:*	Plain='utf-8' html='utf-8'
8.	*X-Resolved-To:*	bob@bob.com
9.	*X-Delivered-To:*	bob@bob.com
10.	*X-Mail-From:*	alice@alice.com
11.	*Authentication-Results:*	mta1294.mail.mud.bob.com from=alice.com; domainkeys=neutral (no sig); from=alice.com; dkim=neutral (no sig)
12.	*Received:*	from 127.0.0.1 (EHLO mailbox-us-s-7b.tariq.com) (a2.b2.c2.d2) by mta1294.mail.mud.bob.com with SMTP; Tue, 30 Nov 2010 07:36:34 -0800
13.	*Received:*	from MTBLAPTOP (unknown [a1.b1.c1.d1]) (Authenticated sender: tariq@tariq.com) by mailbox-us-s-7b.tariq.com (Postfix) with ESMTPA id 8F0AE139002E for <bob@bob.com>; Tue, 30 Nov 2010 15:36:23 +0000 (GMT)
14.	*From:*	"Allice" <Alice@a.com>
15.	*Subject:*	A Sample Mail Message
16.	*To:*	"Bob Jones" <bob@bob.com>
17.	*Content-Type:*	multipart/alternative; charset="utf-8"; boundary="KnRl8MgwQQWMSCW6Q5=_HgI2hwAdah5NLY"
18.	*MIME-Version:*	1.0
19.	*Content-Transfer-Encoding:*	8bit
20.	*Content-Length:*	511
21.	*Reply-To:*	"Smith" <smith@smith.com>
22.	*Organization:*	Alices Organization
23.	*Date:*	Tue, 28 Nov 2010 21:06:22 +05.30
24.	*Return-Receipt-To:*	smith@smith.com

25.	*Disposition-Notification-To:*	jones@jones.com
26.	*Message-Id:*	<20101130153623.8F0AE139002E@mailbox-us-s-7b.tariq.com>

Sumber: (Banday, 2011c)

Berikut adalah penjelasan dari masing-masing *field* dari Tabel 2.1:

1. X-Apparently-To: merupakan alamat email penerima, baik itu menggunakan To, Cc, atau Bcc.
2. Return-Path: berisi alamat email kotak surat yang ditentukan oleh pengirim dalam perintah MailFrom. Alamat ini dapat dipalsukan jika tidak ada mekanisme otentikasi di server pengirim seperti yang ditunjukkan pada contoh di baris ke-2. Keaslian *field* ini tidak dapat ditentukan hanya melalui analisis *header*.
3. Received-SPF: nilai yang ditunjukkan menentukan bahwa email berasal dari dimain yang tidak memiliki catatan SPF atau belum menjadi pengirim yang ditunjuk.
4. X-Spam-Ratio: skor spam yang dihitung oleh perangkat lunak penyaring spam dari server penerima atau MUA. Jika rasio ini melebihi ambang batas yang ditentukan sebelumnya, maka email akan diidentifikasi sebagai spam.
5. X-Originating-IP: menunjukkan alamat IP MTA terakhir dari server SMTP pengirim, yang telah mengirimkan email ke server penerima, yaitu bob@bob.com. Dalam contoh di atas alamat IP-nya adalah a2.b2.c2.d2 seperti yang ditunjukkan pada baris ke-5. Alamat email penerima juga tercantum pada *field Received*.
6. X-Sieve: menentukan nama dan versi dari sistem penyaring pesan yang digunakan. Hal ini berkaitan dengan bahasa scripting yang digunakan untuk menentukan kondisi untuk penyaringan dan penanganan pesan. Dalam contoh di atas, perangkat lunak yang digunakan untuk menyaring pesan adalah CMU Sieve versi 2.3
7. X-Spam-Charsets: menentukan kumpulan karakter yang digunakan untuk menyaring pesan. Pada contoh di atas, server Bob menggunakan 8-bit Unicode Transformation Format (UTF). UTF ini memiliki properti khusus yang kompatibel dengan ASCII.
8. X-Resolved-To: berisi alamat email kotak surat yang dikirimkan oleh MDA dari server penerima. Dalam banyak kasus, value X-Resolved-To sama dengan X-Delivered-To. Pada contoh di atas, email tersebut dikirim oleh MDA dari server Bob.
9. X-Mail-From: menentukan alamat email dari kotak surat yang ditentukan oleh pengirim dalam perintah MailFrom, yang pada contoh di atas adalah alice@alice.com.

10. Authentication-Result: mengindikasikan bahwa mtal1294.mail.mud.bob.com menerima email dari domain alice.com yang tidak memiliki DomainKeys signature maupun DKIM signature.
11. Received pada baris ke-12: *field Received* kedua yang berisi informasi jejak yang menunjukkan bahwa IP 127.0.0.1 sebagai alamat IP mesin yang mengirim pesan. Mesin ini sebenarnya adalah mailbox-us-s-7b.tariq.com dan memiliki alamat IP a2.b2.c2.d2. Perintah SMTP EHLO digunakan untuk mengirim email tersebut. Email diterima oleh mta1294.mail.mud.bob.com menggunakan SMTP. Email diterima pada Selasa, 30 November 2010 pada pukul 07:36:34. Jamnya 8 jam lebih cepat dari GMT.
12. Received pada baris ke-13: *field Received* pertama, menunjukkan informasi jejak bahwa MTBLAPTOP sebagai nama mesin pengirim email. Mesin ini tidak dikenal oleh penerima tapi memiliki alamat IP a1.b1.c1.d1 dan tariq@tariq.com adalah pemilik kotak surat yang mengirim pesan. MTA harus mengikuti beberapa mekanisme otentikasi untuk mengidentifikasi pengguna kotak suratnya. Jika tidak, tidak mungkin untuk memasukkan alamat kotak surat pengirim terotentikasi dengan *field Received*. Email diterima oleh mailboc-us-s-7b-tariq.com dengan protokol ESMTPA yang telah menjalankan program *Postfix*. Email tersebut adalah untuk bob@bob.com dan ID-nya 8F0AE139002E, diterima pada Selasa, 30 November 2010 pukul 15:36:23. Jam telah diatur sesuai dengan GMT.
13. From, Subject, dan To: menunjukkan alamat email pengirim, subjek/judul pesan, dan alamat email penerima. *Field Subject* dan *To* ditentukan oleh pengirim dan *From* diambil oleh sistem dari pengguna yang masuk saat ini. *Field From* dapat dengan mudah dipalsukan seperti contoh diatas yang telah dipalsukan untuk menunjukkan bahwa pengirim email adalah Alice@a.com dengan nama Alice.
14. Content-Type, MIME-Version, Content-Transfer-Encoding, dan Content-Length: merupakan penjelasan dari jenis konten MIME, penyandian transfer, versi dan panjang sehingga MUA dapat melakukan decoding yang tepat untuk dapat menyampaikan pesan kepada penerima.
15. Reply-To: berisi alamat email yang digunakan untuk menerima email balasan dari penerima email. Pada email yang dipalsukan, *field* ini sangat mungkin ditulis dengan alamat email acak yang tidak terkait dengan pengirim sehingga bisa menyebabkan kebocoran informasi.
16. Organization: mengindikasikan organisasi yang diklaim oleh pengirim yang pada contoh di atas adalah Alices Organization.

17. Date: mengindikasikan tanggal dan waktu saat email dibuat dan dikirimkan. Pada contoh di atas, email dikirim pada Selasa, 28 November 2010 pukul 21:06:22 +05.30, yang mana tidak sesuai dengan *field Received* sebelumnya.
18. Return-Receipt-To: menunjukkan alamat email, MSA, MTA, dan MDA yang digunakan untuk mengirim notifikasi apakah pesan tersebut berhasil dikirimkan atau tidak. Pada contoh di atas, alamat yang disebutkan adalah alamat acak yang mungkin milik beberapa pengguna yang tidak terkait dengan pengirim,
19. Disposition-Notification-To: menunjukan alamat email, MUA yang harus digunakan ketika mengirimkan pesan yang menunjukan bahwa pesan telah ditampilkan. Pada contoh di atas, alamat yang dituliskan adalah alamat acak yang memang milik beberapa pengguna yang mungkin tidak terkait dengan pengirim.
20. Message-Id: berisi identitas yang unik dari sebuah pesan yang merupakan kombinasi dari nomor unik dan nama domain dari server pengirim.

2.4 Forensik Email

Forensik email adalah sebuah studi tentang sumber dan isi sebuah email sebagai bukti untuk mengidentifikasi pengirim dan penerima pesan, tanggal dan waktu transmisi, catatan terperinci dari transaksi sebuah email, maksud dan tujuan pengirim email, pemindaian port, dan identifikasi penipuan email (Banday, 2011b). Forensik email juga dapat didefinisikan sebagai suatu tindakan pengamanan, pengecekkan, serta penelusuran terhadap email palsu atau terhadap bukti-bukti kejahatan yang menggunakan email (Karsono, 2012). Pengertian lainnya dijelaskan bahwa yang termasuk aktivitas forensik email adalah pemeriksaan dan pengungkapan informasi penting yang terdapat pada email (Devendran et al., 2015).

Investigasi forensik terhadap email dapat dilakukan dengan memeriksa *header* dan *body* dari sebuah email. Proses investigasi email dilakukan dengan memeriksa alamat email pengirim, memeriksa protokol inisiasi pesan (HTTP, SMTP), memeriksa ID pesan, dan memeriksa alamat IP pengirim. Beberapa aspek lain yang dapat mempengaruhi tahapan investigasi forensik email, yaitu: format penyimpanan email, ketersediaan Salinan cadangan email, dan protokol yang digunakan untuk mengirim email (Devendran et al., 2015).

Ada beberapa teknik investigasi dalam forensik email yang dapat dilakukan untuk mengungkapkan kasus kriminal yang melibatkan email, yaitu: *header analysis*, *bait tactics*, *server investigation*, *software embedded identifiers*, dan *sender mailer fingerprints.* Teknik *header analysis* merupakan suatu teknik analisis yang dilakukan pada metadata yang terdapat pada *header* sebuah email. Metadata tersebut berisi informasi mengenai pengirim

dan/atau jalur yang dilalui oleh pesan selama dalam perjalanan menuju alamat email yang dituju. Beberapa di antaranya mungkin telah dipalsukan untuk menyembunyikan identitas pengirim. Analisis *header* dilakukan dengan menganalisis *header email* secara detail dan menemukan korelasi dari setiap *field* pada *header* (Banday, 2011b).

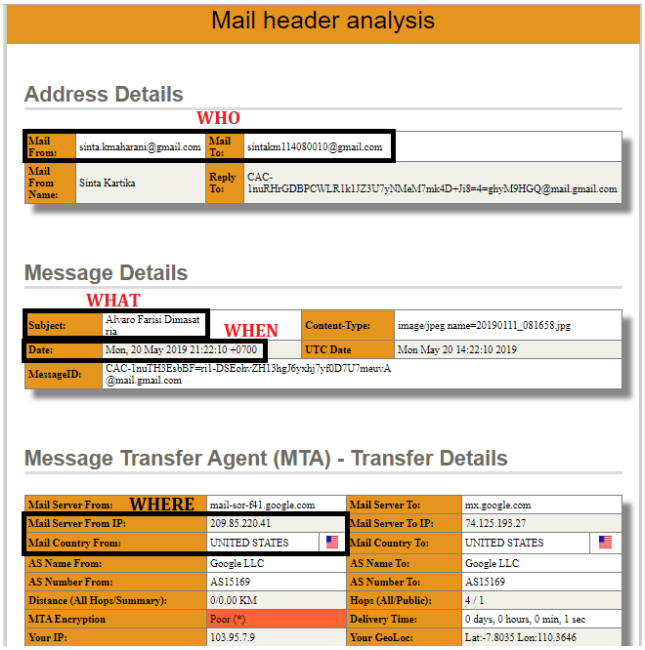
Sebelum membuat *tool* email forensik ini, telah dilakukan komparasi beberapa *tools* analisis *header email* yang telah tersedia secara *online*. Hal ini bertujuan untuk mengetahui informasi apa saja yang dapat diekstraksi dari *header email*. Setiap *tool* yang diujikan menampilkan informasi yang berbeda-beda. Poin yang diperhatikan dalam melakukan komparasi ini adalah informasi apa saja yang ditampilkan, apakah sudah dapat menjawab pertanyaan 5W1H (*Who*, *What*, *When*, *Where*, *Why*, dan *How*).

Proses komparasi *tools* dilakukan terhadap 14 *tools* forensik email yang tersedia secara gratis di internet dengan menggunakan 1 *header email* yang sama (terdapat pada Lampiran). Berikut adalah hasil dari 14 *tools* yang dikomparasi:

2.4.1 Mail Header Analysis (mailheader.org)

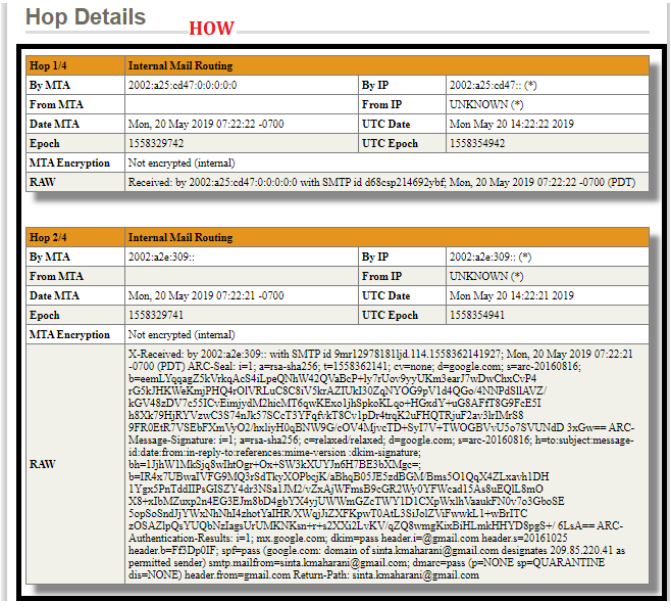
Tool mailheader.org menganalisis *header email* kemudian menampilkan informasi yang lengkap, meliputi: alamat email pengirim dan penerima, subjek email, tanggal email dikirim, *messageID*, MTA (*Mail Transfer Agent*), skor *spam*, dan detail *hop*. Jika merujuk pada konsep 5W1H di atas, *tool* mailheader.org telah dapat menjawab pertanyaan-pertanyaan: *Who*, *What*, *When*, *Where*, dan *How*. Informasi *How* yang ditampilkan oleh *tool* ini berasal dari *field Received* dan *X-Received*.

Gambar 2.2 menunjukkan bahwa *tool* Mail Header Analysis dapat menampilkan informasi dari *header email* berupa alamat email pengirim dan penerima (menjawab *Who*), subjek dari email (menjawab *What*), tanggal pengiriman email (menjawab *When*), dan alamat IP dari *server* pengirim email dan lokasinya (menjawab *Where*). Selain itu ditampilkan pula informasi MessageID dari email yang dikirimkan, nama *server* pengirim dan penerima email, dan lama waktu pengiriman. Terlihat bahwa email dikirimkan dari alamat sinta.kmaharani@gmail.com kepada sintakm114080010@gmail.com dengan subjek "Alvaro Farisi Dimasatria". Email dikirimkan pada 20 Mei 2019 jam 21:22 WIB.



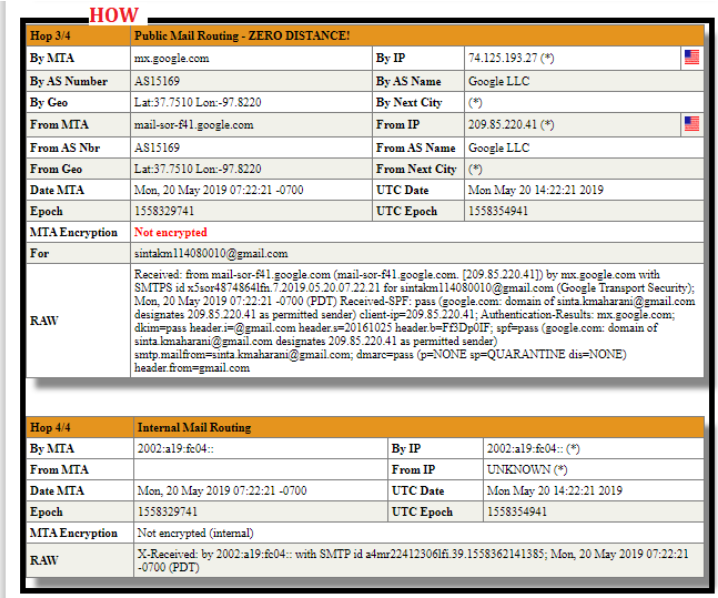
Gambar 2.2 Tampilan hasil analisis *tool* Mail Header Analysis

Informasi mengenai proses pengiriman email dari pengirim hingga sampai di penerima (menjawab *How*) ditunjukkan pada Gambar 2.3. Terlihat dari Gambar 2.3, *tool* Mail Header Analysis menampilkan *hop* dari *field Received* atau *X-Received* yang teratas pada *header email*. *Field Received* atau *X-Received* yang teratas merupakan *server* SMTP terakhir yang dikunjungi oleh email. *Hop* 1 menunjukkan bahwa email diterima oleh MTA *server* SMTP di sisi penerima dengan alamat IP 2002:a25:cd47:0:0:0:0:0, sedangkan *hop* 2 menunjukkan bahwa email sebelumnya telah diterima oleh MTA *server* SMTP dengan alamat IP 2002:a2e:309::.



Gambar 2.3 Tampilan hasil analisis *tool* Mail Header Analysis

Gambar 2.4 menunjukkan *hop* 3 dan 4 dari email yang dikirimkan dari sinta.kmaharani@gmail.com tadi. *Hop* 3 menunjukkan email diterima oleh MTA mx.google.com dengan alamat IP 74.125.193.27 dari MTA mail-sor-f41.google.com dengan alamat IP 209.85.220.41. *Hop* 4 menunjukkan email tadi diterima oleh MTA *server* SMTP di sisi pengirim dengan alamat IP 2002:a19:fc04::.



Gambar 2.4 Tampilan hasil analisis *tool* Mail Header Analysis

2.4.2 Email Header Analyzer (mxtoolbox.com)

Tool mxtoolbox.com ini memindahkan informasi dari *header email* ke dalam bentuk tabel, sesuai dengan *field* dan *value* dari masing-masing *field*. Pertanyaan *Who*, *What*, *When*, dan *How* dapat dijawab oleh *tool* ini. Tampilan hasil analisis dari *tool* ini ditunjukkan pada Gambar 2.5 dan Gambar 2.6. Gambar 2.5 memperlihatkan informasi dari *header email* yang ditampilkan oleh *tool* Email Header Analyzer berupa proses pengiriman email dari pengirim hingga sampai di penerima (menjawab *How*). Informasi yang ditampilkan ini, hanya berasal dari *field Received* dan ditampilkan dari *Received* terbawah. *Hop* 1 menunjukkan bahwa email dari MTA mail-sor-f41.google.com dengan alamat IP 209.85.220.41 oleh MTA mx.google.com. *Hop* 2 menunjukkan bahwa email diterima oleh MTA dengan alamat IP 2002:a25:cd47:0:0:0:0:0.

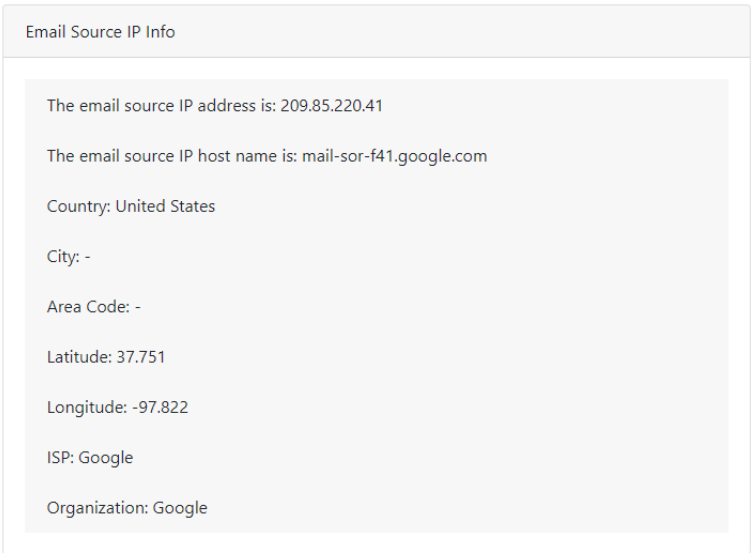
Gambar 2.5 Tampilan hasil analisis *tool* Mail Header Analyzer

Gambar 2.6 menunjukkan informasi lainnya yang ditampilkan oleh *tool* Email Header Analyzer adalah alamat email pengirim dan penerima (menjawab *Who*), subjek dari email (menjawab *What*), dan tanggal pengiriman email (menjawab *When*). Terlihat dari Gambar 2.6 bahwa email dikirim dari sinta.kmaharani@gmail.com kepada sintakm114080010@gmail.com dengan subjek "Alvaro Farisi Dimasatria" dan dikirimkan pada 20 Mei 2019 pukul 21:22 WIB. Terdapat informasi Message-ID juga ditampilkan.

Gambar 2.6 Tampilan hasil analisis *tool* Mail Header Analyzer

2.4.3 Email Header Analyzer (whatismyip.com)

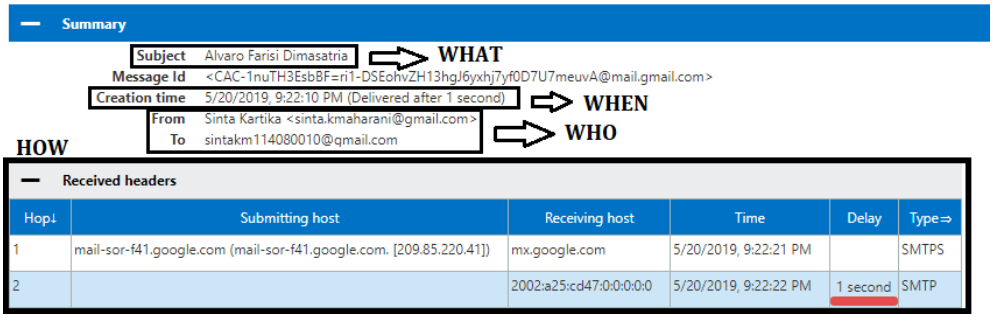
Analisis *header* yang dilakukan oleh *tool* whatismyip.com lebih fokus ke analisis alamat IP yang ada pada *header email*, sehingga *tool* ini hanya menjawab pertanyaan *Where*, yaitu menunjukkan alamat IP *server* pengirim email. Informasi yang ditampilkan berupa alamat IP dari MTA pengirim email, lokasi dari alamat IP tersebut beserta koordinat garis bujur dan garis lintangnya. Tampilan hasil analisis *tool* Email Header Analyzer tersebut dapat dilihat pada Gambar 2.7. Dengan menggunakan *header email* yang sama, hasil analisis dari Email Header Analyzer menunjukkan bahwa email dikirim dari *server* dengan alamat IP 209.85.220.41 yang *host name*-nya mail-sor-f41.google.com berada di United States/ Amerika Serikat dengan koordinat garis lintang 37.751 (37^{o} 45' 3.6'' Lintang Utara) dan koordinat garis bujur -97.822 (97^{o} 49' 19.2'' Bujur Barat).



Gambar 2.7 Tampilan hasil analisis *tool* Mail Header Analyzer

2.4.4 Message Header Analyzer (testconnectivity.microsoft.com)

Tool dari Microsoft ini menganalisis *header email* kemudian menampilkan informasinya yang dapat menjawab pertanyaan *Who*, *What*, *When*, dan *How*. Tampilan hasil analisis dari Message Header Analyzer ditunjukkan pada Gambar 2.8. Terlihat bahwa *tool* Message Header Analyzer menampilkan informasi berupa subjek dari email (menjawab *What*), waktu email dikirimkan (menjawab *When*), alamat email pengirim dan penerima (menjawab *Who*) dan proses pengiriman email dari pengirim hingga sampai di penerima (menjawab *How*). Informasi *How* ini hanya diambil dari *field Received* dan ditampilkan dari *Received* terbawah.

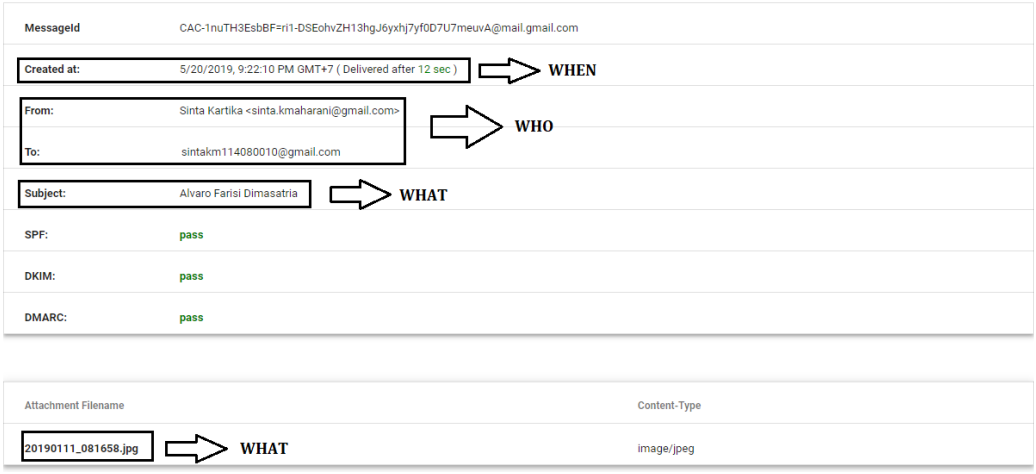


Gambar 2.8 Tampilan hasil analisis *tool* Message Header Analyzer

2.4.5 Message Header (toolbox.googleapps.com)

Informasi hasil analisis *header email* yang ditampilkan oleh *tool* ini telah menjawab pertanyaan *Who*, *What*, *When*, dan *How*. Kelebihan *tool* milik Google ini adalah dapat menampilkan informasi file lampiran yang ada pada email, sedangkan pada *tool* lain yang

dikomparasi, informasi ini tidak ada. Tampilan hasil analisis dari *tool* dapat dilihat pada Gambar 2.9 dan Gambar 2.10. Gambar 2.9 memperlihatkan informasi yang dapat ditampilkan oleh *tool* adalah waktu email dikirimkan (menjawab *When*), alamat email pengirim dan penerima (menjawab *Who*), serta subjek dari email dan file lampiran yang ada pada email (menjawab *What*).



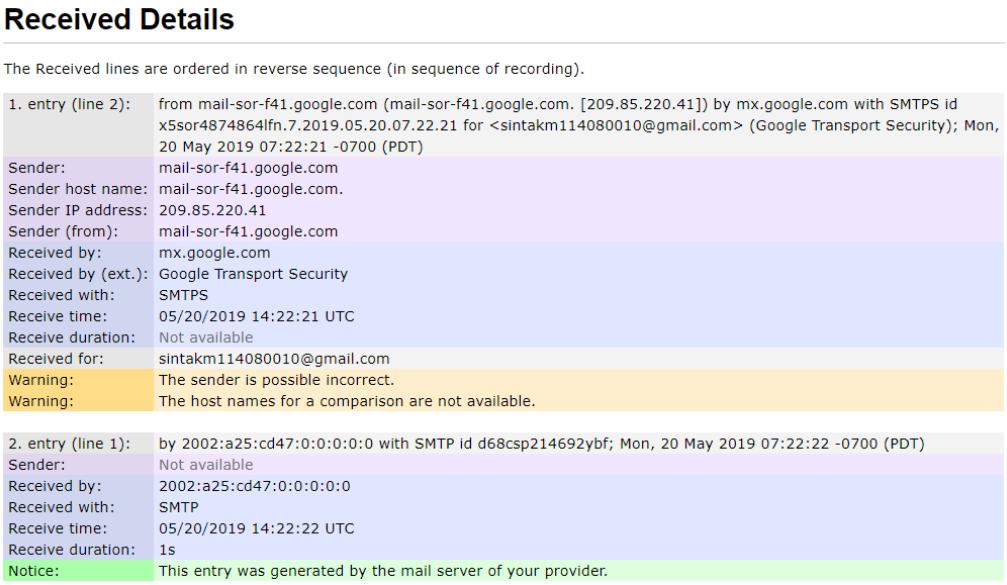
Gambar 2.9 Tampilan hasil analisis *tool* Message Header

Gambar 2.10 menunjukkan informasi lain yang ditampilkan oleh *tool* Message Header, yaitu proses pengiriman email dari pengirim hingga sampai di penerima (menjawab *How*). Untuk menjawab *How*, *tool* Message Header mengambil dari *field Received* dan *X-Received*. Pembacaan *field Received* dan *X-Received* dilakukan dari yang terbawah.

Gambar 2.10 Tampilan hasil analisis *tool* Message Header

2.4.6 E-Mail Header Analyzer (gaijin.at)

Tool E-Mail Header Analyzer dari Gaijin.at ini hanya terfokus untuk menerjemahkan *field Received* yang ada pada *header email*, sehingga hanya menjawab pertanyaan *How*. Gambar 2.11 dapat dilihat hasil analisis *header email* dari *tool* E-Mail Header Analyzer yang menampilkan informasi mengenai proses pengiriman email dari pengirim hingga sampai di penerima (menjawab *How*). Pertanyaan *How* ini dijawab dengan mengambil *field Received* dan dibaca dari yang paling bawah.



Received Details

The Received lines are ordered in reverse sequence (in sequence of recording).

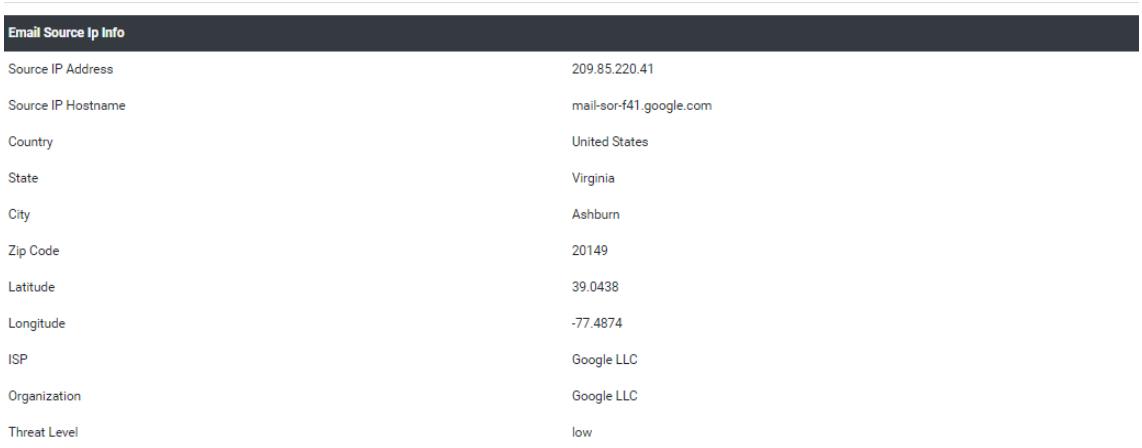
1. entry (line 2):	from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41]) by mx.google.com with SMTPS id x5sor4874864lfn.7.2019.05.20.07.22.21 for <sintakm114080010@gmail.com> (Google Transport Security); Mon, 20 May 2019 07:22:21 -0700 (PDT)
Sender:	mail-sor-f41.google.com
Sender host name:	mail-sor-f41.google.com.
Sender IP address:	209.85.220.41
Sender (from):	mail-sor-f41.google.com
Received by:	mx.google.com
Received by (ext.):	Google Transport Security
Received with:	SMTPS
Receive time:	05/20/2019 14:22:21 UTC
Receive duration:	Not available
Received for:	sintakm114080010@gmail.com
Warning:	The sender is possible incorrect.
Warning:	The host names for a comparison are not available.

2. entry (line 1):	by 2002:a25:cd47:0:0:0:0:0 with SMTP id d68csp214692ybf; Mon, 20 May 2019 07:22:22 -0700 (PDT)
Sender:	Not available
Received by:	2002:a25:cd47:0:0:0:0:0
Received with:	SMTP
Receive time:	05/20/2019 14:22:22 UTC
Receive duration:	1s
Notice:	This entry was generated by the mail server of your provider.

Gambar 2.11 Tampilan hasil analisis *tool* E-Mail Header Analyzer

2.4.7 Trace Email (dnschecker.org)

Sama seperti whatismyip.com, *tool* ini berfokus pada analisis alamat IP yang ada pada *header email*, sehingga hanya menjawab pertanyaan *Where*. Informasi yang dijabarkan cukup lengkap meliputi ISP, koordinat garis bujur dan lintang, kota, serta negara dari alamat IP tersebut. Gambar 2.12 menunjukkan informasi hasil analisis dari *header email* yang sama, yaitu alamat IP *server* pengirim email adalah 209.85.220.41 yang berlokasi di kota Ashburn, negara bagian Virginia, Amerika Serikat dengan kode pos 20149.



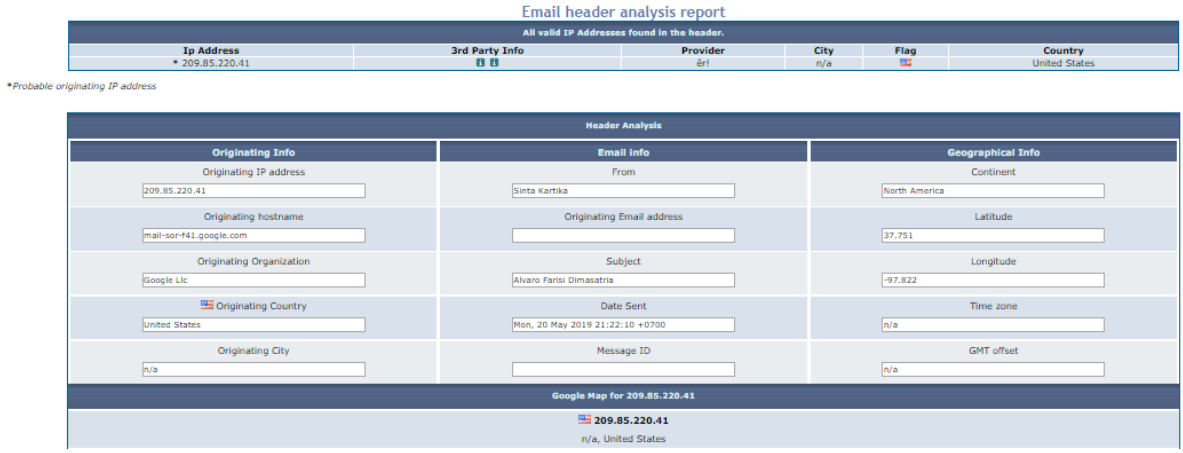
Email Source Ip Info	
Source IP Address	209.85.220.41
Source IP Hostname	mail-sor-f41.google.com
Country	United States
State	Virginia
City	Ashburn
Zip Code	20149
Latitude	39.0438
Longitude	-77.4874
ISP	Google LLC
Organization	Google LLC
Threat Level	low

Gambar 2.12 Tampilan hasil analisis *tool* Trace Email

2.4.8 Email Header Analysis (iptrackeronline.com)

Tool ini juga berfokus pada informasi alamat IP yang ada pada *header email* seperti 2 *tool* sebelumnya, whatismyip.com dan dnschecker.org, sehingga dapat menjawab pertanyaan

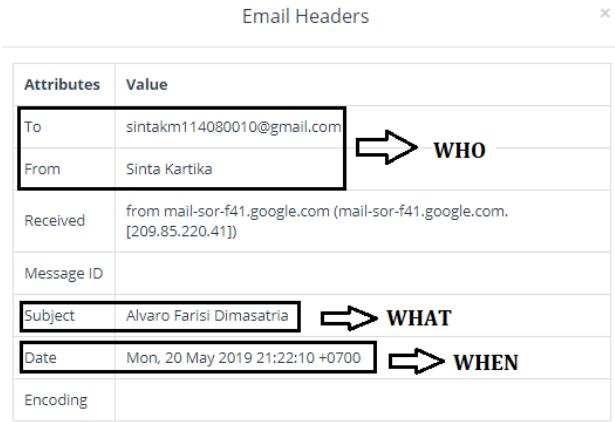
Where. Selain itu, *tool* ini juga menampilkan informasi waktu pengiriman email (menjawab *When*) dan subjek dari email (menjawab *What*). Penjabaran informasinya meliputi koordinat garis lintang dan bujur serta negara dari alamat IP tersebut. Gambar 2.13 menunjukkan tampilan informasi hasil analisis *header email* oleh *tool* Email Header Analysis dari iptrackeronline.com.



Gambar 2.13 Tampilan hasil analisis *tool* Email Header Analysis

2.4.9 Email Header Analyzer (emailheaders.net)

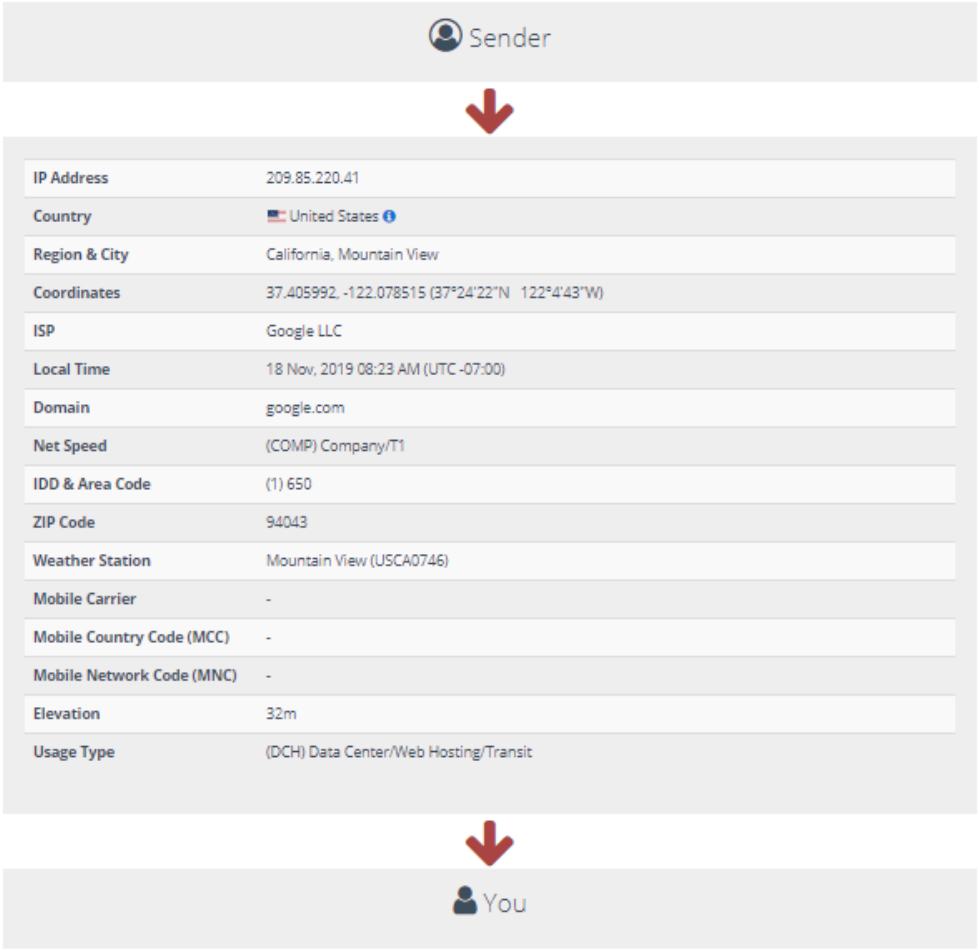
Informasi hasil analisis *header email* yang ditampilkan oleh *tool* ini dapat menjawab pertanyaan-pertanyaan *Who*, *What*, dan *When*. *Tool* Email Header dapat menampilkan informasi alamat email pengirim dan penerima (menjawab *Who*), subjek dari email (menjawab *What*), dan waktu pengiriman email (menjawab *When*). Informasi hasil analisis *header email* tersebut dapat dilihat pada Gambar 2.14.



Gambar 2.14 Tampilan hasil analisis *tool* Email Header Analyzer

2.4.10 Email Header Tracer (ip2location.com)

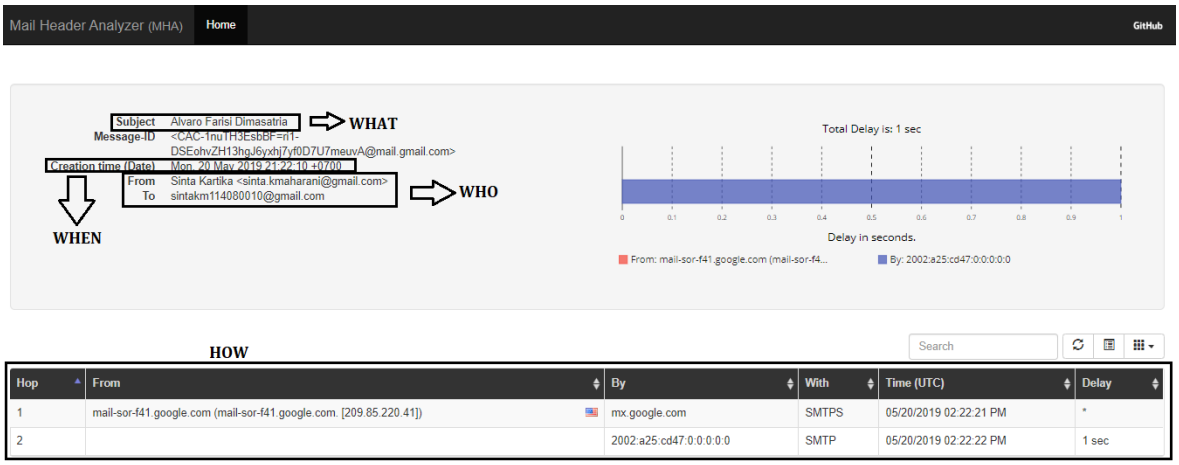
Tool Email Header Tracer fokus menganalisis informasi alamat IP yang ada pada *header email*, sehingga pertanyaan *Where* dapat dijawab oleh *tool* ini. Informasi hasil analisis *header email* yang ditampilkan oleh *tool* ini meliputi alamat IP beserta lokasi alamat IP tersebut, ISP, dan koordinat garis lintang dan bujur dari lokasi alamat IP-nya. Tampilan informasinya dapat dilihat pada Gambar 2.15.



Gambar 2.15 Tampilan hasil analisis *tool* Email Header Tracer

2.4.11 Mail Header Analyzer (mailheaderanalyzer.herokuapp.com)

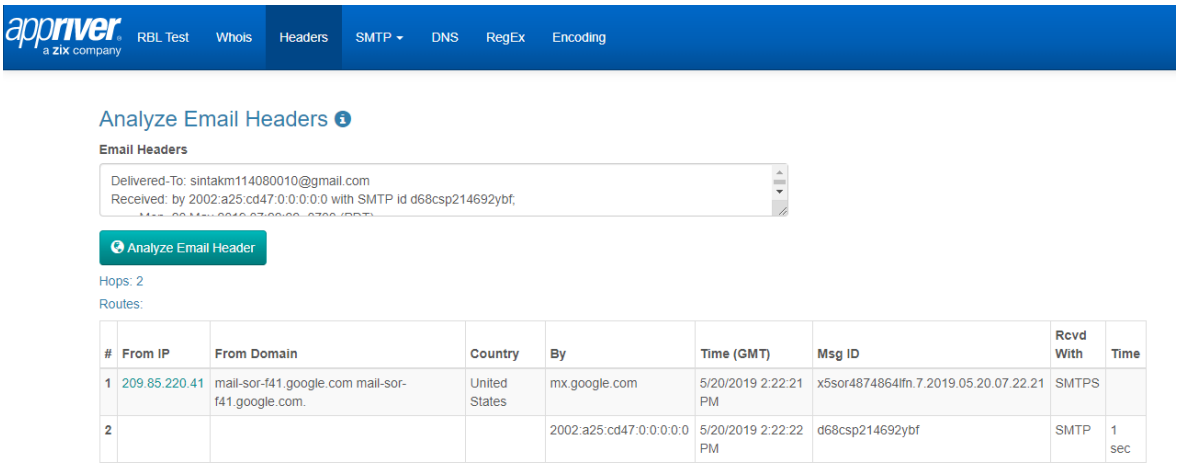
Mail Header Analyzer dari Heroku menganalisis *header email*, kemudian informasi hasil analisisnya dapat menjawab pertanyaan-pertanyaan *Who*, *What*, *When*, *Where*, dan *How*. Gambar 2.16 memperlihatkan informasi hasil analisis *header email* dari *tool* ini, yaitu subjek email (menjawab *What*), waktu pengiriman email (menjawab *When*), alamat email pengirim dan penerima (menjawab *Who*), dan proses pengiriman email hingga diterima (menjawab *How*). Untuk jawaban *How*, *tool* Mail Header Analyzer hanya mengambil dari *field Received*.



Gambar 2.16 Tampilan hasil analisis *tool* Mail Header Analyzer

2.4.12 Analyze Email Headers (tools.appriver.com)

Analisis *header email* yang dilakukan oleh *tool* dari Appriver ini berfokus pada penerjemahan *field Received*, sehingga *tool* ini menjawab pertanyaan *How*. Terdapat informasi tambahan yang ditampilkan oleh *tool* Analyze Email Headers ini, yaitu alamat IP dari *server* pengirim email beserta lokasi negara dari alamat IP tersebut, maka pertanyaan *Where* juga terjawab. Tampilan hasil analisis *header email* dari *tool* ini ditunjukkan pada Gambar 2.17.

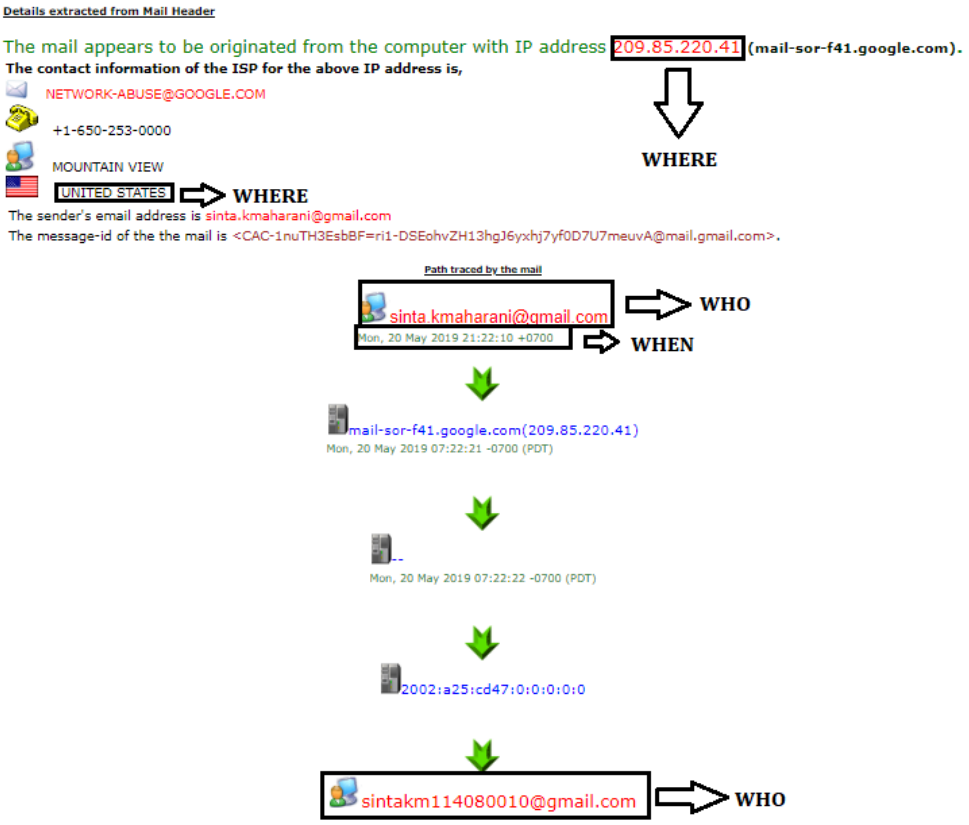


Gambar 2.17 Tampilan hasil analisis *tool* Analyze Email Headers

2.4.13 Online Email Tracer (cyberforensics.in)

Hasil analisis *header email tool* Online Email Tracer dari Cyber Forensics India ini dapat menjawab pertanyaan *Who*, *When*, *Where*, dan *How*. Selain itu, hasil analisisnya dilengkapi dengan ilustrasi proses pengiriman email berdasarkan *hop*-nya. Informasi yang ditampilkan oleh *tool* ini dapat dilihat pada Gambar 2.18 dan Gambar 2.19. Gambar 2.18 menujukkan

informasi hasil ekstraksi *header email* yang meliputi alamat IP dari *server* pengirim dan lokasi alamat IP-nya (menjawab *Where*), alamat email pengirim dan penerima (menjawab *Who*), waktu email dikirimkan (menjawab *When*).



Gambar 2.18 Tampilan hasil analisis *tool* Online Email Tracer

Informasi mengenai proses pengiriman email dari pengirim hingga ke penerima (menjawab *How*) ditunjukkan pada Gambar 2.19. Untuk menjawab *How* ini, *tool* Online Email Tracer mendapatkan informasinya dari *field Received* yang dibaca dari *field Received* terbawah.

HOW

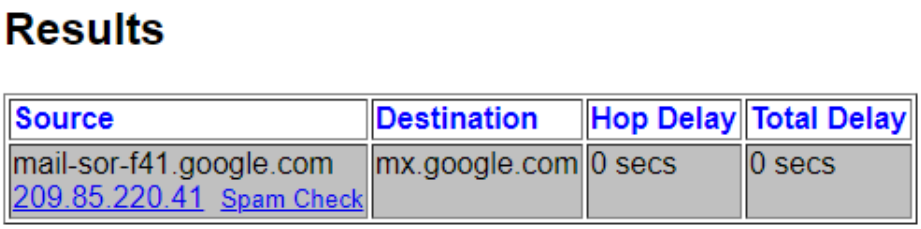
Received By	Received From	Date
sintakm114080010@gmail.com	2002:a25:cd47:0:0:0:0:0	--
2002:a25:cd47:0:0:0:0:0	--	Mon, 20 May 2019 07:22:22 -0700 (PDT)
--	mail-sor-f41.google.com[209.85.220.41]	Mon, 20 May 2019 07:22:21 -0700 (PDT)
mail-sor-f41.google.com[209.85.220.41]	sinta.kmaharani@gmail.com	Mon, 20 May 2019 21:22:10 +0700

Gambar 2.19 Tampilan hasil analisis *tool* Online Email Tracer

2.4.14 Mail Parse (levinecentral.com)

Mail Parse adalah *tool* analisis *header email* dari LevineCentral.com. *Tool* ini melakukan analisis *header email* yang berfokus hanya pada *field Received* saja, sehingga hanya menjawab pertanyaan *How*. *Field Received* yang diambil oleh *tool* ini adalah *field Received*

yang memuat informasi alamat IP. Gambar 2.20 menunjukkan tampilan informasi hasil analisis *header email* dari Mail Parse



Results

Source	Destination	Hop Delay	Total Delay
mail-sor-f41.google.com 209.85.220.41 Spam Check	mx.google.com	0 secs	0 secs

Gambar 2.20 Tampilan hasil analisis *tool* Mail Parse

Berdasarkan hasil komparasi dari 14 *tools* di atas, rancangan *tool* yang akan dibuat adalah dapat menampilkan informasi lengkap yang menjawab pertanyaan *Who*, *What*, *When*, *Where*, dan *How* (4W1H). Selain itu, *tool* juga dapat memberikan tanda peringatan jika *header email* yang diujikan terindikasi sebagai *email fraud* atau *email spoofing*. Perbedaan dari 14 *tools* yang dikomparasi dengan *tool* yang akan dibuat dapat dilihat pada Tabel 2.2.

Tabel 2.2 Hasil Komparasi *Tools* Forensik Email

No.	Tool	Who		What		When		Where		How	Indikasi
		Pengirim	Penerima	Subjek	Lampiran	Dikirim	Diterima	Alamat IP	Lokasi	Hop	*Email Fraud/ Spoofing*
1.	Mail Header Analysis	✓	✓	✓	×	✓	×	✓	✓	✓	×
2.	Email Header Analyzer (MxToolbox)	✓	✓	✓	×	✓	×	×	×	✓	×
3.	Email Header Analyzer (whatismyip.com)	×	×	×	×	×	×	✓	✓	×	×
4.	Message Header Analyzer	✓	✓	✓	×	✓	×	×	×	✓	×
5.	Message Header	✓	✓	✓	✓	✓	×	×	×	✓	×
6.	E-Mail Header Analyzer (gaijin.at)	×	×	×	×	×	×	×	×	✓	×
7.	Trace Email (Header Analyzer)	×	×	×	×	×	×	✓	✓	×	×

No.	Tool	Who		What		When		Where		How	Indikasi *Email Fraud/ Spoofing*
		Pengirim	Penerima	Subjek	Lampiran	Dikirim	Diterima	Alamat IP	Lokasi	Hop	
8.	Email Header Analysis	×	×	✓	×	✓	×	✓	✓	×	×
9.	Email Header	✓	✓	✓	×	✓	×	×	×	×	×
10.	Email Header Tracer	×	×	×	×	×	×	✓	✓	×	×
11.	Mail Header Analyzer	✓	✓	✓	×	✓	×	✓	✓	✓	×
12.	Analyze Email Headers	×	×	×	×	×	×	✓	✓	✓	×
13.	Online EMailTracer	✓	✓	✓	×	✓	×	✓	✓	✓	×
14.	Mail Parse	×	×	×	×	×	×	×	×	✓	×
	Usulan penelitian (Mail Header Extractor)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

2.5 Kejahatan Email

Email merupakan layanan internet yang banyak digunakan sebagai media komunikasi antara satu pengguna dengan yang lainnya, baik secara personal maupun secara kelompok/ perusahaan. Email dapat menjadi media bagi penjahat untuk melakukan pencurian data pribadi dari penerima email. Beberapa contoh kejahatan email:

1. *Fraud*

   Email fraud adalah penipuan yang sengaja dibuat untuk keuntungan pribadi pelaku atau untuk merusak orang lain melalui media email. Biasanya isi email adalah penawaran investasi dengan iming-iming modal rendah dengan keuntungan besar atau penjualan barang-barang berharga dengan harga sangat rendah. Beberapa contoh bentuk *email fraud* adalah *spoofing* dan *phishing*.

   a) *Email spoofing,* adalah pemalsuan email yang dilakukan dengan mengubah isi *field* yang ada pada *header email,* sehingga tampak berasal dari sumber yang benar-benar sah.

   b) *Email phishing,* adalah bentuk kejahatan email yang bertujuan untuk memperoleh data/ informasi pribadi dari penerima email. *Email phishing* biasanya berisi bujukan kepada penerimanya untuk mengisi data pribadi dengan detail.

2. *Spamming*

   Email spam adalah email yang dikirimkan secara massal dan berulang yang tidak diinginkan oleh penerima. *Email spam* ini biasanya bersifat komersial tetapi bisa juga termasuk di dalamnya berupa email berantai.

3. *Bombing*

   Email bombing adalah usaha mengirim email dalam jumlah sangat banyak dalam upaya membuat *mailbox* menjadi *overflow* atau membanjiri *server* email sehingga menyebabkan serangan DoS (*Denial of Service*).

2.6 Penelitian Terkait

Penelitian dalam bidang forensik email dengan memanfaatkan *header email* telah banyak dilakukan. Ada beberapa teknik yang dapat digunakan untuk melakukan forensik email, yaitu: *header analysis, bait tactics, server investigation, network device investigation, software embedded identifiers,* dan *sender mail fingerprint* (Banday, 2011b). Pada penelitian lain dirancang sebuah algoritma untuk mendeteksi pemalsuan tanggal pada email dengan

cara menganalisis *header email*. Algoritma yang diusulkan ini memanfaatkan *field* "*Date*", "*Resent-Date*", dan "*Received*" pada *header email* dan digunakan pada sisi *server* penerima email (Banday, 2011a).

Usulan algoritma dalam melakukan analisis forensik terhadap waktu dan tanggal email yang telah dipalsukan adalah dengan membaca informasi yang terdapat pada *header* dan menganalisis *field* yang terkait, yaitu: "*Date*" (berisi tanggal dan waktu pengiriman), "*Received*" yang pertama (berisi alamat IP dari server yang menerima email dari pengirim beserta tanggal dan waktu penerimaannya), dan "*Received*" yang terakhir (berisi alamat IP dari server terakhir yang menerima email dari pengirim beserta tanggal dan waktu penerimaannya) (Mishra, Pilli, & Joshi, 2012). Algoritma forensik email lainnya dibuat dengan tiga tingkat, dimulai dengan mengumpulkan barang bukti yang kemudian diikuti dengan melakukan analisis *header*, analisis *log server* email, dan analisis *image* komputer lokal. Algoritma ini bertujuan untuk mengetahui dengan pasti asal-usul sebuah email (Msongaleli & Kucuk, 2018).

Algoritma forensik email lainnya diusulkan untuk pendeteksian *email spoofing* dengan membandingkan *field* "*From*" dan "*Message-ID*" pada header untuk menentukan apakah telah terjadi pemalsuan alamat email pengirim dan dengan membandingkan *field* "*Date*" dan "*Received*" yang terakhir pada header untuk menentukan apakah terjadi pemalsuan waku pengiriman email (Hoiriyah, 2016).

Beberapa perangkat lunak *open source* telah dikembangkan untuk membantu investigator dalam melakukan investigasi forensik email. Beberapa contoh perangkat lunak, seperti eMailTrackerPro, EmailTracer, Adcomplain, Aid4Mail Forensic, AbusePipe, AccessData's FTK, EnCase Forensic, FINALeMAIL, Sawmill-GroupWise, Forensics Investigation Toolkit (FIT), dan Paraben (Network) E-mail Examiner, dapat membantu mempelajari sumber dan isi email sehingga serangan dari intrusi dapat diselidiki. *Tools* tersebut dapat melakukan analisis *header* dan inspeksi perangkat jaringan secara otomatis untuk membantu mempercepat proses investigasi (Banday, 2011c).

Studi komparatif perbandingan 5 *tools* yang populer dan digunakan secara luas dalam bidang forensik email dilakukan dengan menilai 9 kriteria dari masing-masing *tools*, yaitu: syarat input *file*, opsi pencarian, informasi yang dapat diekstraksi, kemampuan *recovery*, format *file* email yang didukung, dukungan visualisasi, sistem operasi yang didukung, perangkat tambahan yang didukung, dan format ekspor yang didukung. Kelima *tools* tersebut adalah MailXaminer, Aid4Mail, Digital Forensic Framework, eMailTrackerPro, dan Paraben E-Mail Examiner. Berdasarkan kriteria "informasi yang diekstraksi", hasil studi

menunjukkan bahwa *tools* MailXaminer, Aid4Mail, dan Digital Forensic Framework hanya dapat menunjukkan rincian pesan, tanggal dan waktu dari suatu email. Sedangkan *tool* eMailTrackerPro dapat menampilkan alamat IP pengirim pesan beserta lokasi geografisnya serta mampu menemukan penyedia layanan jaringan (ISP) pengirim dan menampilkan tabel *routing* yang dapat mengidentifikasi jalur antara pengirim dan penerima email. *Tool* Paraben E-Mail Examiner dapat menampilkan informasi yang tersedia berdasarkan hasil pemeriksaan *header* dan isi email, termasuk lampiran (Devendran et al., 2015).

Rangkuman penelitan terkait di atas ditunjukkan pada Tabel 2.3.

Tabel 2.3 Penelitian Terkait

Paper utama	**Domain Penelitian**	**Poin yang dianalisis**	**Metode/*Tools***	**Keterangan**
(Banday, 2011b)	Teknik investigasi forensik email.	-	-	Teknik investigasi forensik email: *header analysis*, *bait tactics*, *server investigation*, *network device investigation*, *software embedded identifiers*, *sender mailer fingerprints*.
(Banday, 2011a)	Algoritma untuk mendeteksi dan mencegah pemalsuan tanggal pada email.	*Field header* email: *Date*, *Resent-Date*, *Received*.	Membandingkan nilai dari ketiga *field header* tersebut dengan *current date* di server penerima.	Jika ditemukan perbedaan, email akan dideteksi sebagai email palsu dan akan mengirimkan pemberitahuan ke pengirim.
(Mishra et al., 2012)	Algoritma untuk melakukan analisis forensik dari email yang tanggal dan waktunya dipalsukan dengan membaca *header* dan menganalisis *field* yang berkaitan dengan tanggal dan waktu.	*Field header* email: *Date*, *Received* yang pertama, *Received* yang terakhir.	Membandingkan waktu dan tanggal kirim dengan waktu dan tanggal terima dengan beberapa margin yang telah ditentukan.	Jika hasilnya berbeda, maka email telah dipalsukan.
(Msongaleli & Kucuk, 2018)	Algoritma *three-tiered* untuk investigasi kriminal dan	*Header* email, *log* server email, dan *image*	Melakukan analisis terhadap *header* email, *log*	Dari hasil studi kasus, dapat diketahui pengirim dan

Paper utama	Domain Penelitian	Poin yang dianalisis	Metode/*Tools*	Keterangan
	penyelesaian sengketa yang berkaitan dengan email.	komputer lokal (pengirim atau penerima email).	server email, dan *image* dari komputer lokal.	kredibilitas dari email jahat dan yang disengketakan.
(Hoiriyah, 2016)	Algoritma pendeteksian pemalsuan email.	*Field header* email: *From, Message-ID, Date*, dan *Received* yang terakhir.	Membandingkan *field From* dan *Message-ID* serta *field Date* dan *Received*.	Jika nilai dari *field From* dan *Message-ID* berbeda, dideteksi alamat email pengirim telah dipalsukan. Jika nilai dari *field Date* dan *Received* berbeda, dideteksi waktu pengiriman telah dipalsukan.
(Banday, 2011c)	Beberapa *tools* yang dapat digunakan investigator untuk melakukan investigasi forensik email.	Fitur-fitur dari masing-masing *tools*.	eMailTrackerPro, EmailTracer, Adcomplain, Aid4Mail Forensic, AbusePipe, AccessData's FTK, EnCase Forensic, FINALeMAIL, Sawmill-GroupWise, Forensic Investigation Toolkit (FIT), Paraben (Network) E-mail Examiner	*Tools* tersebut dapat melakukan analisis *header* secara otomatis dan inspeksi perangkat jaringan secara otomatis untuk membantu mempercepat proses investigasi.

Paper utama	Domain Penelitian	Poin yang dianalisis	Metode/*Tools*	Keterangan
(Devendran et al., 2015)	Studi komparatif membandingkan 5 *tools* forensik email dengan 9 kriteria yang telah ditetapkan.	syarat input *file*, opsi pencarian, informasi yang ditampilkan, kemampuan *recovery*, format *file* email, visualisasi, sistem operasi, perangkat tambahan, format ekspor *file*.	• MailXaminer • Aid4Mail • Digital Forensic Framework • eMailTrackerPro • Paraben E-Mail Examiner	Berdasarkan kriteria "informasi yang ditampilkan", MailXaminer, Aid4Mail, dan Digital Forensic Framework dapat menunjukkan rincian pesan, tanggal dan waktu. EMailTrackerPro dapat menampilkan alamat IP pengirim pesan serta lokasi geografisnya. Paraben E-Mail Examiner mampu menampilkan *header* dan isi email, termasuk lampiran.
Usulan penelitian	Membaca *header email*.	*Field* pada *header email*: *From*, *To*, *Cc*, *Bcc*, *Received-SPF*, *Date*, *X-Received*, *Subject*, dan *Received*.	Membuat *tool* yang dapat membaca *header* dan melakukan *parsing* data dari *field* yang telah ditentukan.	*Tool* yang dihasilkan diharapkan dapat memetakan informasi yang menjawab pertanyaan: • *Who*, siapa pengirim dan penerima email? • *Where*, di mana letak server dari pengirim email?

Paper utama	Domain Penelitian	Poin yang dianalisis	Metode/*Tools*	Keterangan
				• *When*, kapan email dikirim dan diterima? • *What*, apa subjek dari email? • *How*, bagaimana perjalanan email dari pengirim hingga sampai ke penerima?