Jurnal Teknologi Informasi dan Komunikasi
Vol: 13 No 02 2022 **E-ISSN: 2477-3255**
Diterima Redaksi: 05-10-2022 | Revisi: 30-10-2022 | Diterbitkan: 15-11-2022

Live Forensics Analysis Of Malware Identified Email Crimes To Increase Evidence Of Cyber Crime

Yudhi Prawira[1], Samsudin[2]
[1,2,\]Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sumatera Uttara
[1,2,]Jl. Lap. Golf, Kp. Tengah, Kab. Deli Serdang, Sumatera Utara
e-mail: [1]yudhiprawira00@gmail.com, [2]samsudin@uinsu.ac.id

Abstract

Now days Email is the most important aplplication on the internet, this make email one of the industry's most targeted sector for commiting cyber crimes. Email phishing and spam not only harm many parties but also consumes a lot of network bandwidth. Most spam are emotet malware. Trojan malware that targets internet users financial system to steal financial information and personal data by sending phishing. In this research, digital forensics analysis email crimes identified malware using live forensics and tools analyze digital evidence of email content, as wall as offVise, Wireshark, and Procmon to analyze malware activities. The results of the investigation of the email content carried out using software found digital evidence that could be used as a reference that attachment downloaded by the victim was Emoted type malware, when the victim opened it, this malware will be installed automatically on the victim's computer.

.

Keywords: *Digital Forensics, Email, Malware Emotet, live Forensics, Diital Proof.*

Analisis Live Forensics Email yang Teridentifikasi Malware untuk Menetapkan Evidence Kejahatan Cyber

Abstrak

Email telah menjadi aplikasi paling penting di internet, ini membuat email menjadi salah satu most targeted industry sector dalam kejahatan cyber. Email phishing dan spam tidak hanya banyak merugikan berbagai pihak tetapi juga menghabiskan banyak bandwidth jaringan. Sebagian besar email spam adalah malware emotet, malware ini bertujuan untuk mencuri informasi keuangan dan data pribadi dengan mengirimkan email phishing. Pada penelitian ini, analisis digital forensik email yang teridentifikasi malware menggunakan metode live forensics dan menggunakan tools Eml-Viewer untuk menganalisa bukti digital dari konten email, serta OffVise, Wireshark, dan Procmon untuk menganalisis aktivitas malware. Hasil dari Investigasi konten email yang dilakukan dengan menggunakan software Eml-viewer menemukan bukti digital yang bisa dijadikan acuan bahwa email tersebut merupakan email palsu, dan hasil dari

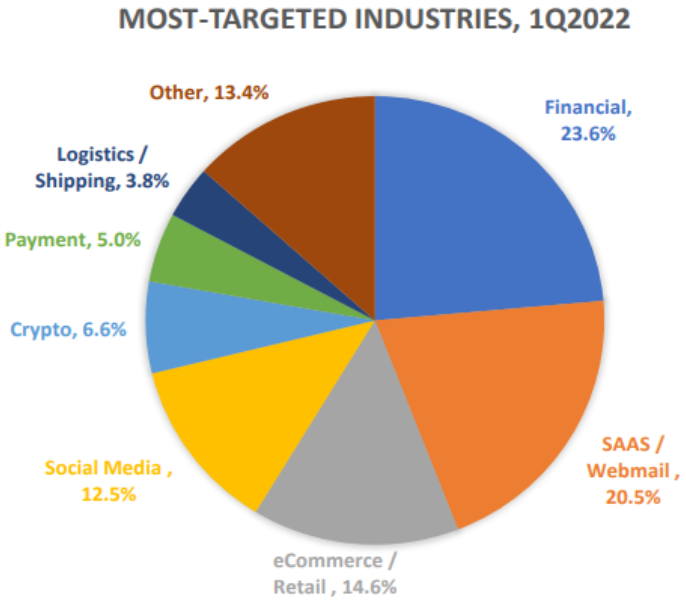
analisis malware ditemukan bahwa Attachment email yang di download oleh korban merupakan malware jenis Emotet, ketika korban membuka pada komputer nya, maka malware ini akan terinstall secara otomatis di komputer korban.

Kata kunci: *Digital Forensics, Email, Malware Emotet, Live Forensics, Digital Proof*

1. Pendahuluan

Pesatnya perkembangan teknologi informasi dan komunikasi telah berdampak pada semua aspek sosial masyarakat [1]. Dalam satu dekade terakhir, penggunaan internet sangat berkembang pesat. Namun, karena internet menjadi bagian dari kegiatan sehari-hari, kejahatan dunia maya juga meningkat [2].Kejahatan dunia maya adalah pelanggaran yang hanya dapat dilakukan dengan menggunakan komputer, jaringan komputer atau bentuk teknologi informasi komunikasi lainnya [3]. Menurut Freeh Penjahat dunia maya menyerang berbagai target peribadi dan publik di seluruh dunia, dalam hal ini di antaranya beberapa investigasi peretasan berhasil menangkap para pelakunya [4].

Anti Phishing Working Group (APWG) pada tanggal 7 juni 2022 kuartal pertama merilis data informasi *Most Targeted Industry Sector*, bahwa pada kuartal pertama tahun 2022, anggota APWG OpSec Security menemukan serangan *phishing* pada email masih mendominasi pada urutan kedua dengan serangan *phishing* sebanyak 20.5% pada kuartal pertama [5].



Gambar 1. APWG Trends Report Q1 2022

Email telah menjadi aplikasi paling penting di internet yang berguna untuk melakukan komunikasi melalui pesan, mengirim dokumen, bahkan mencatat transaksi dan semakin banyak digunakan baik itu oleh perseorangan maupun perusahaan, namun dikarenakan proses transmisi datanya cukup rumit, jaminan data yang dikirim dapat dipertanyakan, bahkan dapat terjadi kemungkinan pemalsuan email ataupun serangan oleh para peretas yang dapat merugikan berbagai pihak [6]. Ini juga mengakibatkan kerugian finansial yang tak terhitung banyak pengguna yang telah jatuh kedalam korban peipuan internet dan praktik penipuan *spammer* lainnya yang mengirim email yang berpura-pura dari perusahaan terkemuka dengan tujuan untuk membujuk individu agar mengungkapkan informasi pribadi yang *sensitive* seperti kata sandi, nomor verifikasi

https://doi.org/10.31849/digitalzone.v13i2.11570

bank dan angka kartu kredit [7]. Email spam tidak hanya membuang waktu pengguna, tetapi juga menghabiskan banyak bandwidth jaringan, dan mungkin menyertakan malware sebagai file yang dapat dieksekusi [8], ancaman malware yang berkembang juga menjadi sulit untuk diabaikan [9]. Sebagian besar email spam adalah malware emotet [10], Emotet adalah malware Trojan modular yang sangat canggih yang menargetkan sistem keuangan pengguna internet untuk mencuri informasi keuangan dan data pribadi dengan mengirimkan email *phishing* [11].

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 *scientific* (ilmiah) hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut [12]. Bukti digital yang ditemukan dalam kasus sebagian besar dapat langsung dibaca dan dianalisis oleh analisa forensik dan investigator sesuai dengan tahapan forensik [13]. Teknik digital forensik digunakan dengan melakukan analisis komputer atau perangkat lunak digital [14].Data dan informasi yang ada pada RAM dapat diperoleh menggunakan teknik *live* forensics [15], serta bukti digital yang dibutuhkan dapat diperoleh dengan menggunakan teknik *live forensics*. *Live forensics* adalah sebuah metode yang digunakan untuk penanganan kejahatan komputer dan data *recovery* saat sistem komputer sedang berjalan [16].

Penelitian yang dilakukan oleh [17] dengan judul "Rancangan Investigasi Forensik Email Dengan Metode National Institute Of Standards And Technology (NIST)". Pada penelitian ini menggunakan metode NIST dengan pendekatan Header Analysis untuk menginvestigasi kejahatan email, hasilnya adalah penyidik dapat menghasilkan pola pemalsuan email yang berupa subjek, alamat dan tanggal email yang palsu. Pada penelitian yang dilakukan [18] dengan judul "Pelacakan Geolocation Pada Forensik Email Terintegrasi Dengan Twitter Geo-Secial Network" melakukan penelitian guna menentukan prediksi koordinat geolocation (latitude dan longitude) pengirim email yang terhubung dengan media social dengan menggunakan algoritma K-Nears Neighbor, hasil dari penelitian ini adalah forensik email menunjukkan lokasi awal peretas berada dari dugaan lokasi sebesar 141.3 km2 menjadi 5.3 km2. Penelitian terakhir adalah penelitian yang dilakukan oleh [19] dengan judul "*Live Forensics of Tools on Android Device for Email Forensics*" melakukan penelitian dengan menganalisis lalu lintas jaringan di jaringannya langsung dengan menggunakan metode NIST, kemudian melakukan perbandingan alat forensik untuk memperoleh bukti digital. Subjek penelitian ini di fokuskan pada layanan email berbasis android untuk mendapatkan bukti digital sebanyak mungkin pada kedua alat tersebut, hasilnya *networkminer* berhasil mendapatkan port penerima, sedangkan di *Wireshark* tidak ditemukan.

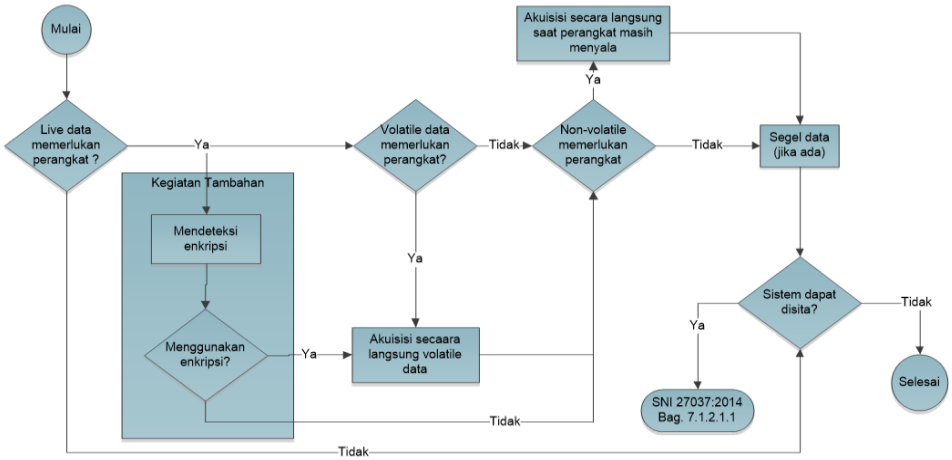
Penelitian ini dibuat dengan memperhatikan penelitian-penelitian yang sudah ada sebelumnya. Perbedaan penelitian ini dengan penelitian sebelumnya yaitu penelitian ini mengangkat studi kasus mengenai email *phishing* yang teridentifikasi malware, teknik yang digunakan untuk mendapatkan data yang terekam pada *Random Access memory* (RAM) adalah teknik *live forensics*, serta menggunakan EML-Viewer, OffVise detection of Malware, Wireshark, dan Procmon sebagai *tools forensics.* Alasan dilakukannya penelitian ini yaitu guna mengetahui karakteristik bukti digital yang di dapat dari aktivitas penggunaan kejahatan email. Tujuan penelitian ini adalah menerapkan dan mengimplementasi teknik *live forensics* pada kejahatan email serta menemukan bukti digital dari investigasi yang dilakukan.

2. Metode Penelitian

Teknik kepustakaan ini merupakan kegiatan yang dilakukan untuk mendukung dalam proses penelitian yang dilakukan, baik mengkaji dan mempelajari sumber literatur dan teori-teori ilmiah, serta wawancara tidak terstruktur yang dilakukan secara tidak langsung kepada salah satu investigator forensik dari Synergy Academy untuk mendukung dari penelitian yang dilakukan.

Pada penelitian ini, metode akuisisi yang akan dilakukan adalah dengan menerapkan metode *live forensics* data *non-volatile* berdasarkan pedoman dan persyaratan dalam Standar Nasional Indonesia (SNI) 27037:2014 [20].

Tahapan metode *live forensics* untuk mengakuisisi bukti digital dalam SNI 270327:2014 di tampilakan pada Gambar 2.



Gambar 2. SNI Acquisition 27037:2014

Ada empat tahap untuk melakukan investigasi forensics sesuai dengan Standar Nasional Indonesia (SNI) 27037:2014. Dimana tahapan tersebut diantaranya adalah :

Identifikasi : ada beberapa proses yang dilakukan pada tahap investigasi, seperti: perencanaan investigasi, persiapan dan pengarahan team, penilaian resiko kemanan TKP, pengamanan TKP, pencarian barang bukti, dan menentukan prioritas barang bukti.

Pengumpulan: ada beberapa proses yang dilakukan pada tahap pengumpulan, seperti: penentuan barang bukti yang disita dan diakuisi di TKP, melakukan penyitaan barang bukti, serta mengumpulkan keterangan-keterangan verbal dari saksi-saksi.

Akuisisi : ada beberapa proses yang dilakukan pada tahap akuisisi, seperti: pemeriksaan aspek barang bukti, penentuan model akuisisi yang dilakukan, pelaksanaan akuisisi, verifikasi hasil akuisisi.

Preservasi : ada beberapa proses yang dilakukan pada tahap preservasi, seperti: memberikan segel barang bukti, melakukanpemeriksaan aspek keamanan pemindahan barang bukti, pemindahan dan penyimpanan barang bukti [21].

2.1. Pengumpulan Data

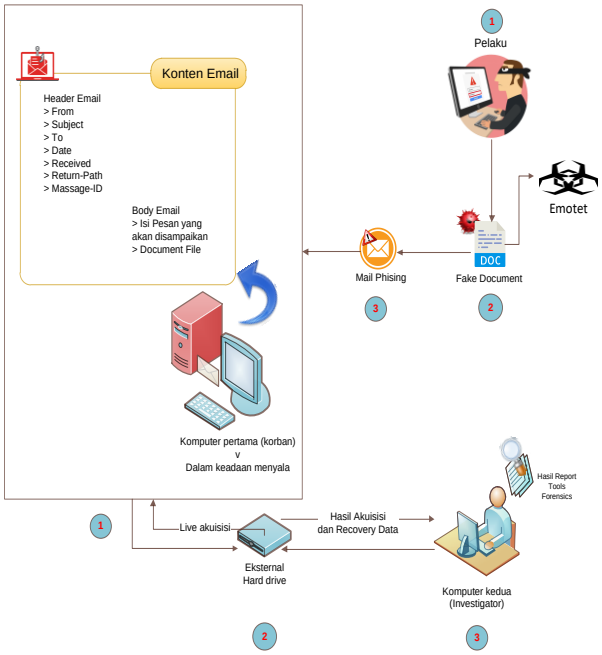
Alat dan bahan yang akan dibutuhkan untuk mendapatkan bukti digital dalam penelitian ini adalah laptop tipe ACER dengan sistem operasi Windows 10 dengan arsitektur 64-bit dan Harddisk eksternal yang akan digunakan untuk penyimpanan *live acquisition*. *Tools forensics* yang akan digunakan untuk *acquisition* data email adalah EML-Viewer, dan selanjutnya untuk melakukan analisis indikasi malware dan aktivitasnnya menggunakan *tools* OffVise detection of Malware, Whireshark, dan Procmon.

https://doi.org/10.31849/digitalzone.v13i2.11570

2.2. Skenario

Dalam penelitian ini membutuhkan skenario kasus kejahatan *cyber* email guna mendapatkan barang bukti digital sebagai langkah menuju tahap analisa. Penelitian ini menggunakan kondisi kejahatan email yang sering terjadi di tengah kehidupan sehari-hari. Gambar ilustrasi skenario proses kejahatan email yang dilakukan oleh pelaku dapat dilihat pada Gambar 3 dan 4, gambar ilustrasi skenario proses analisa yang dilakukan investigator dapat dilihat pada gambar 5.

Gambar 3. Pelaku membuat progam PHP Mailer dan link Phishing



Gambar 4. Skenario Email Live Forensics Recovery

Tahapan yang dilakukan pelaku terhadap korban :

1) Pelaku membuat dan mengirimkan document file pada *Body* email yang isi di dalamnya terdapat malware emotet.
2) Pelaku melakukan dan membuat pemalsuan *Header* email yang seolah-olah pesan tersebut dikirim oleh sumber yang asli.

3) Pelaku menggunakan email *spoofing* untuk mengelabuhi korban dengan *phishing* dan *spamming.*

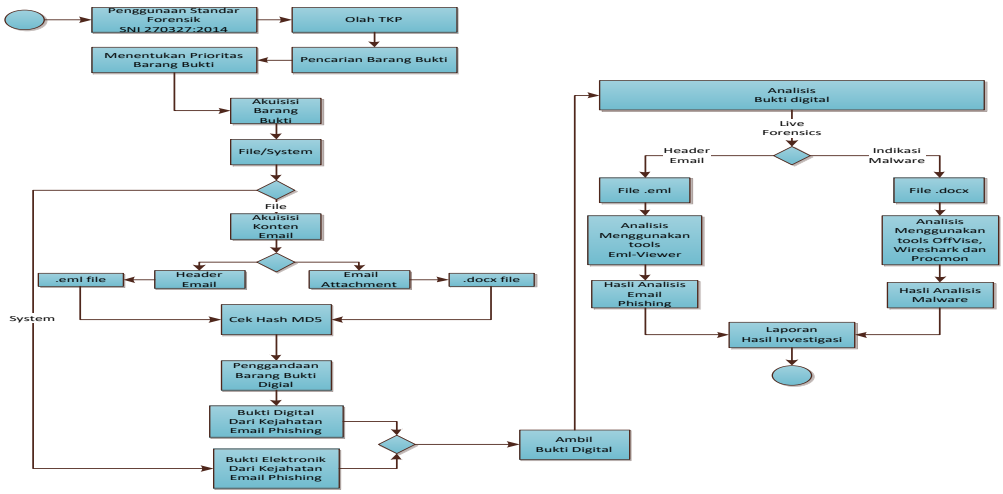
Tahapan yang dilakukan terahadap investigator:

1) Investigator mengkoneksikan Hard disk drive eksternal ke komputer Korban untuk penyimpanan *acquisition* dan *recovery file*.
2) Investigator melakukan analisa file *Header* email menggunakan tools forensics EML-Viewer.
3) Investigator menganalisis document file yang ada pada *Body* email yang diduga malware menggunakan OffVise detection of Malware, Whireshark, dan Procmon.

3. Hasil dan Pembahasan

Penelitian ini dilakukan dengan menggunakan metode *live forensics* menggunakan *harddisk* eksternal untuk mengamankan bukti digital. Berdasarkan skenario yang telah dibuat, investigator akan menganalisis dari bukti digital dari kejahatan email menggunakan tools Eml-viewer, OffVise, Wireshark, dan Procmon.

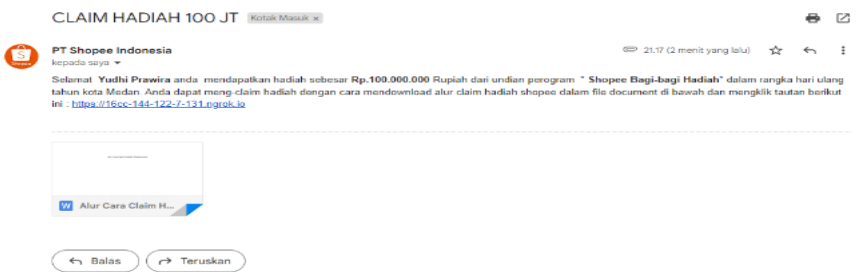
3.1 Alur Penganan Bukti Digital



Gambar 5. Model Algoritma Tahapan Simulasi Penanganan Bukti Digital

a. Identifikasi

Proses identifikasi merupakan kegiatan dalam melakukan pencarian, penggalian, dan pendokumentasian semua hal yang bisa berpotensi menjadi barang bukti digital dari kejahatan cyber. Dalam penelitian ini bukti yang di dapatkan berupa data email dan file document dari komputer korban.



Gambar 6. Bukti Digital Email Phishing Pelaku

https://doi.org/10.31849/digitalzone.v13i2.11570

Tabel 1. Jenis Barang Bukti Kejahatan Email Phishing yang Terindikasi Malware

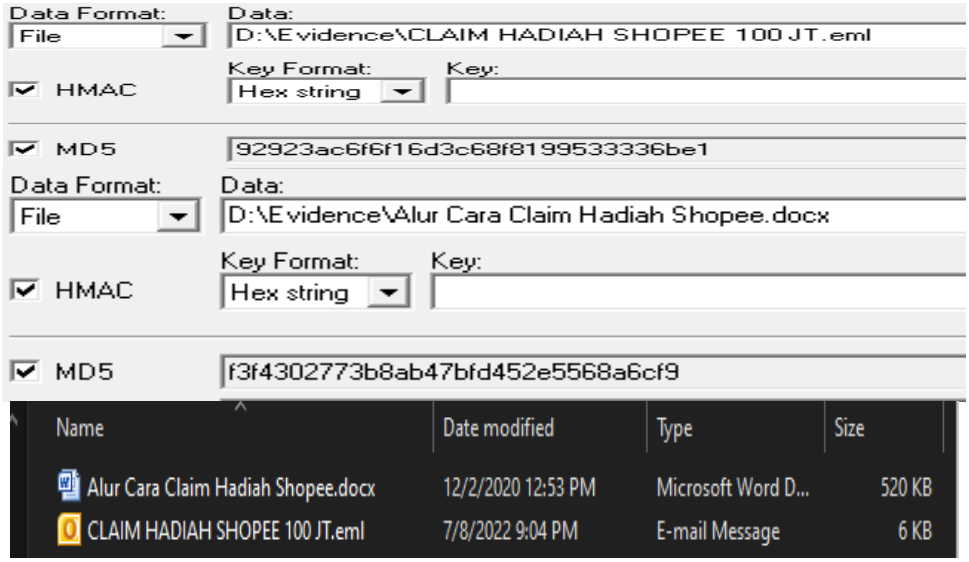
No	Tipe	Nama Barang Bukti	Spesifikasi Barang Bukti
1	Hardware	Laptop Dell Inspiron 13-537	Intel® Core i7-7500u Windows 10 Home Single Language 64 Bit – RAM 8192MB
2	Document	CLAIM HADIAH SHOPEE 30 JT.eml	25 KB
3	Document	Alur cara claim hadiah Shopee.docx	530 KB

b. Pengumpulan

Proses pengumpulan adalah kegiatan penanganan barang bukti digital, memberikan label terhadap barang bukti, mengumpulkan keterangan verbal dari saksi-saksi, dan mengamankan peralatan yang terindikasi menjadi barang bukti, dalam hal ini memindahkan dan melakukan *acquisition* barang bukti kemudian barang bukti ini dipindahkan dari lokasi TKP ke laboratorium agar barang bukti dapat dipastikan aman.

c. Akuisisi

Proses pengumpulan adalah kegiatan penanganan barang bukti digital, memberikan label terhadap barang bukti, mengumpulkan keterangan verbal dari saksi-saksi, dan mengamankan peralatan yang terindikasi menjadi barang bukti, dalam hal ini memindahkan dan melakukan *acquisition* barang bukti kemudian barang bukti ini dipindahkan dari lokasi TKP ke laboratorium agar barang bukti dapat dipastikan aman.



Gambar 7. Verifikasi Hash Dari Hasil Akuisisi Bukti Digital

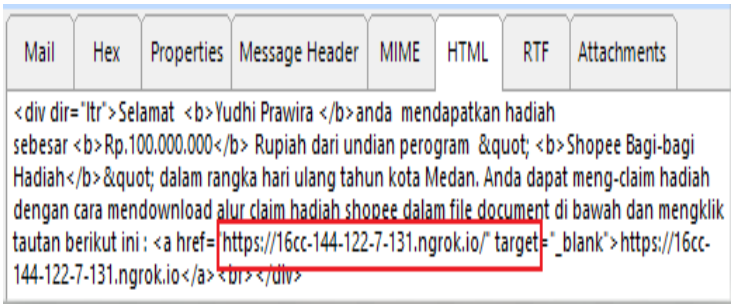
d. Peservasi

Proses preservasi merupakan kegiatan penyegelan, pengamanan, dan pemindahan barang bukti agar barang bukti aman dari tempat TKP ke tempat penyimpanan ataupun laboratorium. Penyimpanan barang bukti yang telah di analisis harus tetap berada di laboratorium atau disimpan di ruang penyimpanan barang bukti kepolisian sampai hakim pengadilan memutuskan apakah barang bukti tersebut bisa di jadikan barang bukti di peradilan.

3.2 Pemeriksaan dan Analisis Bukti Digital

3.2.1 Analisis Konten Email

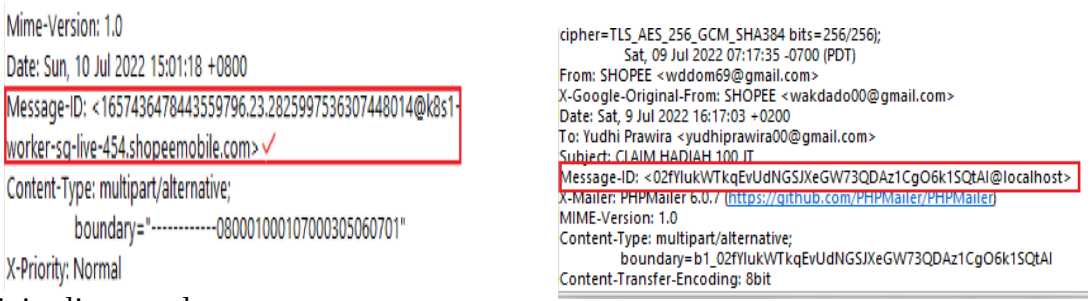
Berdasarkan hasil pemeriksaan yang dilakukan terhadap barang bukti digital, diperoleh hasil bahwa barang bukti tersebut dapat terbaca dengan baik oleh software forensik. Setelah mengananilsis header email menggunakan tools forensik EML-viewer, investigator menemukan informasi mengenai ISP dan kota tempat keberadaan pelaku.



Gambar 8. Analisa Body Email dalam Bentuk HTML

Gambar 8 merupakan Analisa Body Email dalam Bentuk HTML, dalam HTML atribut href menunjukkan URL halaman web tertentu yang akan terbuka setelah mengklik tautan. Ini menunjukkan bahwa pelaku mencoba menjebak korban dengan membuat link atau tautan palsu, ketika link ini di klik biasanya akan tehubung ke situs-situs palsu atau berbahaya. Tautan ini seolah-olah mengantarkan korban ke proses selanjutnya untuk mengisi data pribadi dengan maksud mendapatkan hadiah yang di janjikan oleh pelaku. Dari URL yang dikirimkan oleh pelaku komunikasi ini patut di curigai dan tidak akan aman.

Setelah melakukan analisa pada body email yang terindikasi penipuan, selanjutnya memeriksa informasi header email untuk menentukan apakah pesan email ini asli atau palsu.



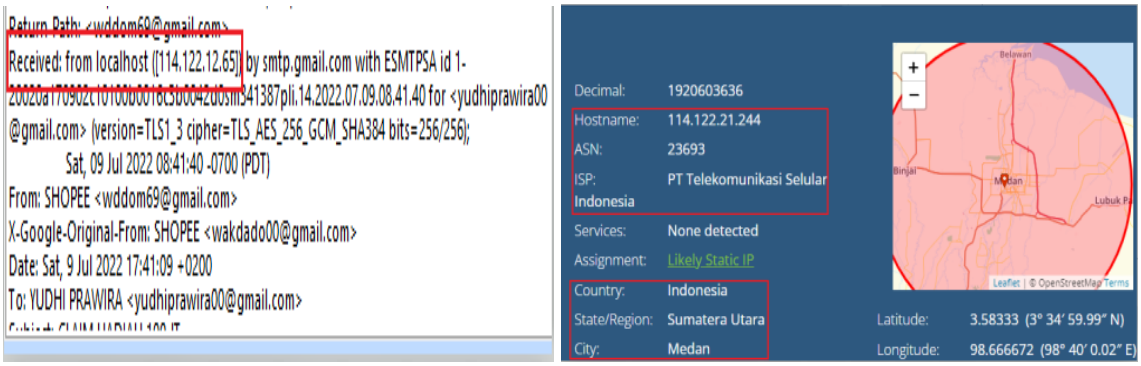
(A) (B)

Gambar 9. Perbandingan Message-ID (A) Email Palsu, (B) Email Asli

Gambar 9 merupakan analisa perbandingan Message-ID email palsu yang di kirim oleh pelaku dengan email yang asli dari perusahaan shopee. Kahadiran localhost setelah simbol @ pada Message-id pada gambar 10 (A) adalah indikator utama bahwa pesan email itu adalah palsu, ini karena nama domain yang ada tidak memenuhi syarat yaitu mail.gmail.com, nama domain juga bisa berbeda sesuai dengan email service providers, seperti yang digunakan oleh perusahan shopee yang asli.

https://doi.org/10.31849/digitalzone.v13i2.11570

Setelah melakukan analisa pada Message-ID untuk menentukan email palsu atau asli, investigasi selanjutnya melakukan pemeriksaan Header Recived untuk mendapatkan alamat IP pelaku dan informasi yang terkait.

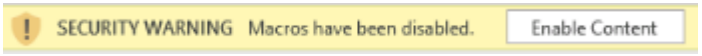


Gambar 10. Analisa Pemeriksaan Header Recived

Gambar 10 merupakan analisa dari pemeriksaan Header Recived, dapat dilihat bahwa bidang header yang diterima mennunjukkan localhost menggantikan nama domain pengirim dimana ini tidak sesuai dengan yang seharusnya yaitu mail-sor-f41.google.com. Dari gambar 10 juga manampilkan alamat IP terkait dari mana pesan itu berasal, ISP yang digunakan, dan lokasi dari pelaku saat mengirim email tersebut.

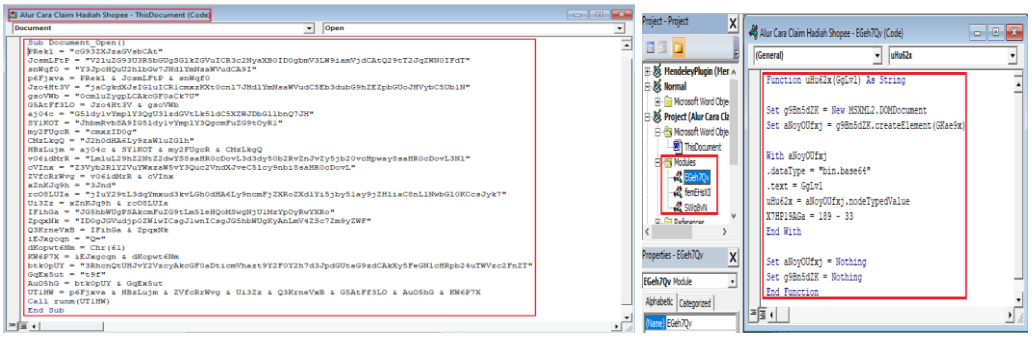
3.2.2 Analisis Indikasi Malware Pada Email Phishing

E-mail Client dan E-mail Server saat ini tidak mengijinkan dan memblokir file arsip (zip, 7zip, rar, dll), binari (executable), script (JavaScript, script VisualBasic) dll. Alasan utama dari tindakan tersebut adalah karena jenis file ini biasanya digunkan untuk serangan cyber. Namun ada beberapa jenis file yang bisa mendukung untuk membuat script tersebut di dalamnya yaitu Microsoft Office Documents. Microsoft office mendukung bahasa scripting yang disebut VBA (Visual Basic for Application) yang jika diaktifkan dapat digunakan untuk kejahatan [22].



Gambar 11. Peringatan Kemanan Macros

Keitka korban membuka dan mengklik aktifkan konten pada file document, maka kode VBA yang ada di dalam file akan mengeksekusi otomatis makro yang ada pada document secara default.

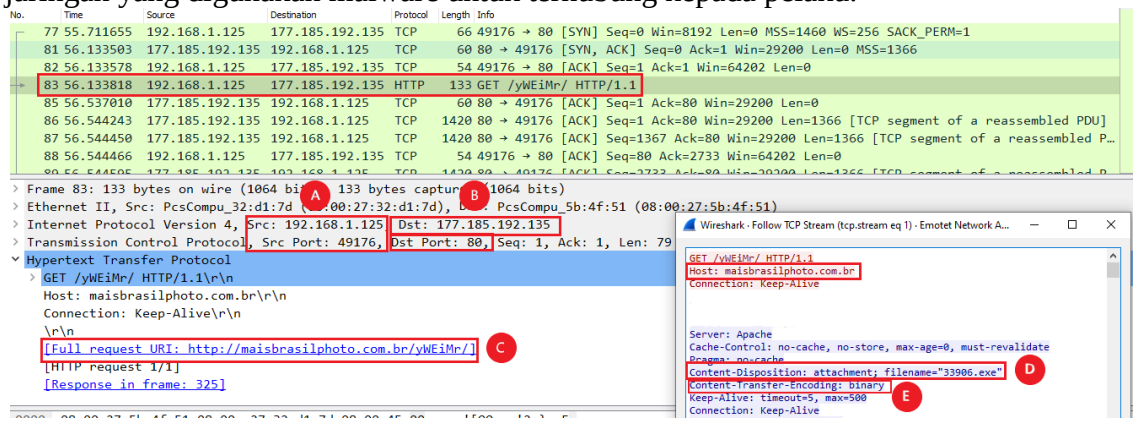


(A) (B)

Gambar 12. Script yang Disematkan Pada File Alur cara claim hadiah Shopee.docx.

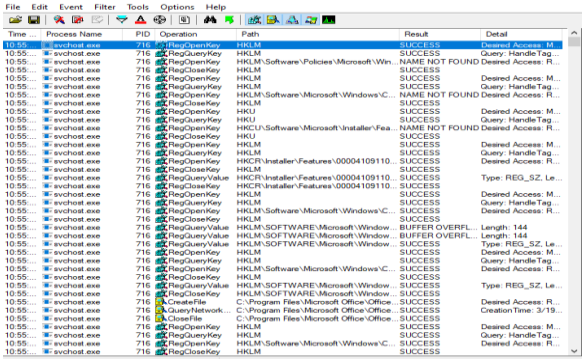
Gambar 12 (A) dan (B) merupakan kode VBA yang di sematkan di file document "Alur cara claim hadiah Shopee.docx". Script ini dibuka dengan fungsionalitas Sub Document_Open, dan berisi banyak string yang terfragmantasi sehingga sulit untuk menganalisis kode untuk mengidentifikasi dan memeriksa script berbahaya yang sebenarnya. Pada gambar 13 (B) lembar kerja Microsoft Visual Basic Aplication terdapat Modul perintah dan inrtuksi lain yang digunakan pada file ini

Setalah melakukan analisa dan pengecekan Marcos pada file document yang terduga malware, selanjutnya investigator melakukan analisis aktivitas malware secara real-time menggunakan tools forensik Wireshark. Investigator menganalisa aktivitas jaringan yang digunakan malware untuk terhubung kepada pelaku.



Gambar 13. Analisis Jaringan Aktivitas Malware

Gambar 13 merupakan aktivitas dan perilaku malware yang terekam pada tools Wireshark. IP 192.168.1.125 pada port 46179 (A) mencoba berkomunikasi dengan situs web https://maisbrasilphoto.com.br dengan hosting di IP 177.185.192.135 melalui port HTTP 80 (B). Ini menjelaskan bahwa kode VBA yang telah disembunyikan di dalam file document "Alur cara claim hadiah Shopee.docx" berisi script untuk mengunduh Emotet, script ini telah dieksekusi dan malware mecoba mengunduh muatan berbahanya dengan berkomunikasi melalui URL https://maisbrasilphoto.com.br/yWEiMr/ (C). File yang di unduh adalah 33096.exe (D), dan objek yang diunduh adalah file binary (E).



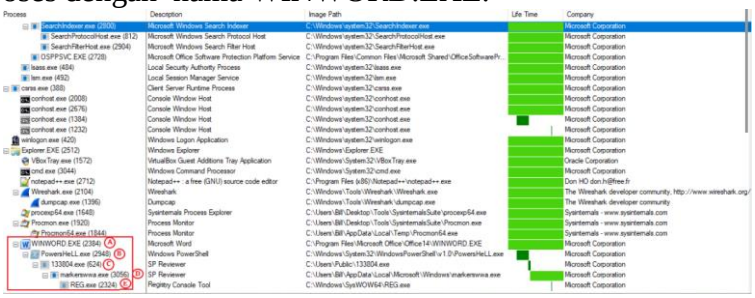
Gambar 14. Process Monitor Pada Malware Emotet

Gambar 14 adalah petunjuk investigasi dari aktivitas Malware yang berjalan di komputer korban, proses analisa ini menggunakan tools procmon64.exe. Tools ini merekam semua proses yang sedang bejalan pada komputer yang terinfeksi malware varian emotet aktif.

Untuk melakukan analisis lebih mendalam mengenai aktivitas Malware Emotet yang berada pada komputer korban, dan karena barang bukti yang di temukan dari

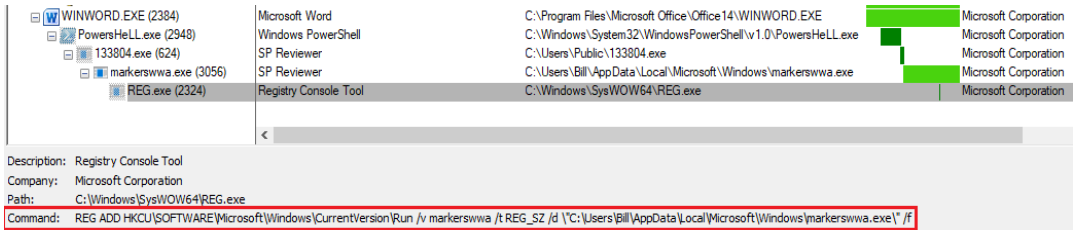
https://doi.org/10.31849/digitalzone.v13i2.11570

attachman email yang di unduh dan di jalankan oleh korban adalah file document Word maka investigator melakukan analisa *Process Tree* yang ada pada tools forensik untuk menemukan proses dengan nama WINWORD.EXE.



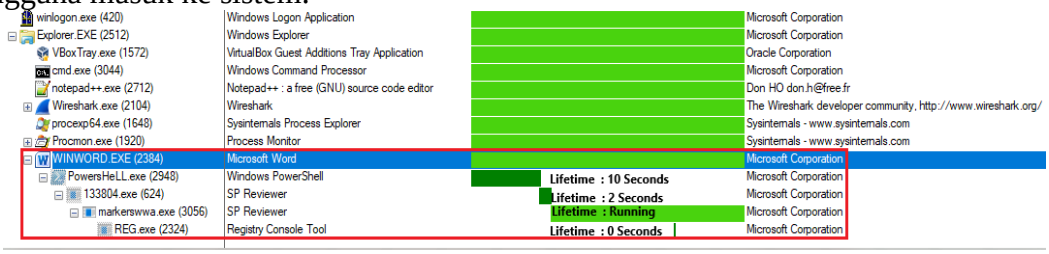
Gambar 15. Process Monitor Pada Malware Emotet

Dapat dijelaskan bahwa hasil *examination* dan Informasi yang di dapat dari gambar 15 adalah pada poin (A) WINWORD.EXE telah mengatur Windows PowerShell sebagi proses turunannya, yang menunjukkan bahwa Kode VBA yang di sembunyikan di dalam file document Word merupakan file berbahaya yang berisi varian Emotet dan berisi script PowerShell. Script PowerShell ini berisi petunjuk tentang URL mana yang harus disambungkan untuk mengunduh payload. File yang diunduh adalah file biner berbahaya dengan nama 33096.exe (B). Setelah file biner dengan nama 33096.exe diunduh melalui script PowerShell yang di sembunyikan, file biner 33096.exe ini juga membuat file biner lain dengan nama markerswwa.exe (C), kemudian markserswwa.exe membuka proses windows lain yaitu REG.exe. REG.exe merupakan *Registry Console Tool* Windows yang berlokasi di C:Windows\SysWOW64. Proses ini sering digunakan oleh pelaku kejahatan malware untuk melakukan aktivitas jahat pada sistem yang terinfeksi malware (D).



Gambar 16. Perintah marksewwa.exe *AutoStart registry key* di OS Windows

Gambar 16 merupakan penjelasan bahwa file biner markerswwa.exe melakukan perintah menggunakan proses REG.exe untuk menambahkan *key value* dibawah HKCU\SOFTWARE\ Microsoft\ Windows\CurrentVersion\Run, untuk bertahan pada mesin komputer yang terinfeksi. Ini adalah perintah *AutoStart registry key* di OS Windows yang akan membuat malware emotet ini berjalan secara ototmatis setiap kali pengguna masuk ke sistem.



Gambar 17. Proses Waktu Yang Dibutuhkan Malware Untuk Mengunduh Muatannya

Setelah file document berbahaya yang berisi pengunduh Emotet dibuka oleh korban, makro yang berisi code VBA akan menjalankan dan memunculkan

PowerShell.exe melalui script berbahaya. Setelahnya PowerShell.exe akan mengunduh payload melalui script, kemudian menjalankan proses file 133804.exe, lalu menghentikan prosesnya dalam waktu 10 detik. File 133804.exe yang berisi payload kemudian membuat file biner baru dengan nama markerswwa.exe, proses ini berjalan degan waktu hanya 2 detik. Selanjutnya proses markerswwa.exe membuka REG.exe untuk mecapai kontrol penuh terhadap mesin komputer, REG.exe membuka dan menutup filenya hanya dalam waktu sekali kejap, hanya file marksewwa.exe yang terus berjalan sementara semua proses induknya ditutup.

Mustafa, dkk [17], membahas mengenai Rancangan Investigasi Forensik Email Dengan Metode *National Institute Of Standards And Technology* (NIST) dan pendekatan *Header Analysis* untuk menginvestigasi kejahatan email, serta *tools* forensik yang digunakan adalah *software* Aid4Mail *forensics*, hasilnya adalah penyidik dapat menghasilkan pola pemalsuan email yang berupa subjek, alamat dan tanggal email yang palsu. Sedangkan dalam penelitian ini membahas mengenai *live forensics* terhadap email yang teridentifikasi malware guna menetapkan *evidence* kejahatan *cyber*, dengan menerapkan metode SNI 270327:2014 dan teknik *live forensics* untuk menginvestigasi dan mengakuisisi bukti kejahatan email, *tools* forensik yang digunakan adalah EML-Viewer, OffVise detection of Malware, Wireshark, dan Procmon. Hasil dari penelitian ini menunjukkan bahwa hasil investigasi yang dilakukan dengan menggunakan bukti digital yang telah diakuisisi dari kejahatan email yang telah terjadi dengan menggunakan teknik *live forensics* bisa mendapatkan bukti digital yang cukup untuk mengetahui jejak digital, cara pelaku mengelabui korbannya, dan motif dari pelaku kejahatan *cyber* tersebut.

4. Kesimpulan

Kejahatan yang sering terjadi melalui email, seperti penipuan, pengancaman dan pembobolan informasi rahasia semakin hari semakin bertambah. Kejahatan email ini berupa *Spamming*, *Scamming*, *Phishing*, *Malware Propagation* , dan *Spoofing*. Berdasarkan hasil penelitian, metode teknik *live forensics* dapat diterapkan untuk akuisisi data dan bukti digital yang ada pada kejahatan email. Proses pemeriksaan dan analisis pada kejahatan email yang teridentifikasi malware dilakukan dengan baik menggunakan tools forensik, yaitu Eml-viewer untuk analisis pada konten email, dan OffVise detection of Malware, Whireshark, serta Procmon untuk melakukan analisis malware dan aktivitasnya di dalam sistem komputer.

Dari hasil investigasi dan analisis bukti digital yang ditemukan menggunakan teknik *live* forensics, investigasi konten email yang dilakukan dengan menggunakan Eml-viewer menemukan bukti digital yang bisa dijadikan acuan bahwa email tersebut merupakan email palsu, faktor utama bukti digital yang menunjukkan ini merupakan tindakan kejahatan adalah terdapat massage-id email yang berbeda dengan alamat email yang asli, bukti digital lainnya yang ditemukan adalah ISP dan alamat IP dari pelaku pengirim email. *Attachment* email yang di download oleh korban merupakan malware jenis Emotet, ketika korban membuka pada komputer nya, maka malware ini akan terinstall secara otomatis. Analisis yang dilakukan pada file document yang di download oleh korban ditemukan bukti bahwa, file ini di sematkan kode VBA (Visual Basic for Application) yang berguna untuk mengunduh file biner berbahaya melalui PowerShelll.exe. Hanya membutuhkan waktu singkat bagi malware untuk mengunduh turunannya dan berkomunikasi dengan pelaku.

https://doi.org/10.31849/digitalzone.v13i2.11570

Bagi penelitian selanjutnya, disarankan untuk melakukan pengujian terhadap alamat IP dari pelaku kejahatan email, agar lebih akurat dan spesifik dalam menentukan lokasi dari pelaku kejahatan email itu sendiri, ini berguna bagi pihak berwajib untuk mempermudah melakukan tahap penyidikan tindak kejahatan cyber.

Daftar Pustaka

[1] M. I. P. Nasution *et al.*, "Biometrics for e-money transaction," *AIP Conf. Proc.*, vol. 2030, no. November, 2018, doi: 10.1063/1.5066942.

[2] R. Ch, T. R. Gadekallu, M. H. Abidi, and A. Al-Ahmari, "Computational system to classify Cyber Crime offenses using machine learning," *Sustain.*, vol. 12, no. 10, 2020, doi: 10.3390/SU12104087.

[3] M. McGuire and S. Dowling, *Cyber Crime: A review of the evidence*, no. October. 2013. [Online]. Available: London, England, United Kingdom

[4] J. X. Li, "Cyber crime and legal countermeasures: A historical analysis," *Int. J. Crim. Justice Sci.*, vol. 12, no. 2, pp. 196–207, 2017, doi: 10.5281/zenodo.1034658.

[5] APWG, "Phishing Activity Trends Report Quarter 4 2021," *apwg.org*, 2022. https://apwg.org/trendsreports/ (accessed Jun. 21, 2022).

[6] H. M. and M. H., "A Survey of Email Service; Attacks, Security Methods and Protocols," *Int. J. Comput. Appl.*, vol. 162, no. 11, pp. 31–40, 2017, doi: 10.5120/ijca2017913417.

[7] E. Gbenga, J. Stephen, H. Chiroma, A. Olusola, and O. Emmanuel, "Heliyon Machine learning for email spam filtering : review , approaches and open research problems," vol. 5, no. February, 2019, doi: 10.1016/j.heliyon.2019.e01802.

[8] T. Gangavarapu, C. D. Jaidhar, and B. Chanduka, "Applicability of machine learning in spam and phishing email filtering: review and approaches," *Artif. Intell. Rev.*, vol. 53, no. 7, pp. 5019–5081, 2020, doi: 10.1007/s10462-020-09814-9.

[9] J. Hemalatha, S. A. Roseline, S. Geetha, S. Kadry, and R. Damaševičius, "An efficient densenet-based deep learning model for Malware detection," *Entropy*, vol. 23, no. 3, pp. 1–23, 2021, doi: 10.3390/e23030344.

[10] J. Page, "Exploring Emotet, an Elaborate Everyday Enigma," *A J. Emerg. Med. Serv. JEMS*, vol. 14, no. 8, pp. 1–25, 2019.

[11] D. Kalla and S. Kuraku, "Emotet Malware – A Banking Credentials Stealer," *IOSR J. Comput. Eng.*, vol. 22, no. 4, pp. 31–40, 2020, doi: 10.9790/0661-2204023140.

[12] M. N. Al-azhar, *Digital Forensic Practical Guidlines for Computer Investigation*. Jakarta, 2012. [Online]. Available: https://lmsspada.kemdikbud.go.id/mod/page/view.php?id=57379

[13] A. P. Saputra and N. Widiyasono, "Analisis Digital Forensik pada File Steganography (Studi kasus : Peredaran Narkoba)," *J. Tek. Inform. dan Sist. Inf.*, vol. 3, no. 1, pp. 179–190, 2017, doi: 10.28932/jutisi.v3i1.594.

[14] R. A. K. N. Bintang, R. Umar, and U. Yudhana, "Perancangan perbandingan live forensics pada keamanan media sosial Instagram, Facebook dan Twitter di Windows 10," *Pros. SNST ke-9 Tahun 2018 Fak. Tek. Univ. Wahid Hasyim*, vol. 1, no. 1, pp. 125–128, 2018.

[15] I. Riadi, S. Sunardi, and M. E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *J. Tek. Elektro*, vol. 10, no. 1, pp. 18–22, 2018, doi: 10.15294/jte.v10i1.14070.

[16] Soni, Y. Prayudi, B. Sugiantoro, D. Sudyana, and H. Mukhtar, "Server Virtualization Acquisition Using Live Forensics Method," vol. 190, pp. 18–23, 2019, doi: 10.2991/iccelst-st-19.2019.4.

[17] Mustafa, I. Riadi, and R. Umar, "Rancangan Investigasi Forensik Email Dengan Netode National Institute Of Standards And Technology (NIST)," vol. 1, no. 1, pp. 121–124, 2018.

[18] N. H. Ardhi, "Pelacakan geolocation pada forensik email terintegrasi dengan twitter geo-social network," *repository.uinjkt.ac.id*, 2020, [Online]. Available: https://repository.uinjkt.ac.id/dspace/bitstream/123456789/53623/1/NAUFAL HERDYPUTRA ARDHI-FST.pdf

[19] R. Umar, I. Riadi, and B. F. Muthohirin, "Live forensics of tools on android devices for email forensics," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 4, pp. 1803–1809, 2019, doi: 10.12928/TELKOMNIKA.v17i4.11748.

[20] *Badan Standarisasi Nasional. SNI 27037:2014 tentang Teknologi Informasi-Teknik Keamanan-Pedoman Identifikasi, pengumpulan, Akuisisi, dan Preservasi Bukti Digital*. Jakarta, 2014.

[21] A. R. Supriyono, B. Sugiantoro, Y. Prayudi, and K. Kunci, "eksplorasi bukti digital pada smart router menggunakan metode live forensics," vol. 10, no. 02, pp. 38–45, 2019.

[22] M. Lupascu, D. T. Gavrilut, and D. Lucanu, "An overview of obfuscation techniques used by malware in visual basic for application scripts," *Proc. - 2018 20th Int. Symp. Symb. Numer. Algorithms Sci. Comput. SYNASC 2018*, pp. 280–287, 2018, doi: 10.1109/SYNASC.2018.00051.