Forensik Digital Pengiriman E-Mail Spam Terhadap Keamanan Cyber Di Indonesia

Rezki Rusydi[1)*], Billy Hendrik[2)], Yassirli Amri[3)]
[1*,2)]Fakultas Ilmu Komputer Universitas Putra Indonesia YPTK Padang,
[3)] Universitas Muhammadiyah Sumatera Barat

rezkirusydi1@gmail.com, yassirliamri09@gmail.com

Abstrak

Internet merupakan bagian dari perkembangan teknologi, dimana internet memberikan banyak dampak, baik positif maupun negatif. Saat ini masalah privasi di internet juga telah menjadi sebuah permasalahan hukum yang pelik, hal ini dikarenakan cukup banyak permasalahan terkait privasi, namun tidak semua negara di dunia mengatur masalah privasi di internet.Sebagai sarana berkomunikasi internet telah mengenalkan e-mail yang memberikan kemudahan dan kepraktisannya. Namun pada perkembangannya e-mail ini memiliki dampak merugikan bagi para penggunanya dalam bentuk e-mail spam. Segi perbuatannya, pengiriman e-mail spam ini cukup banyak merugikan, bahkan melanggar privasi. Beberapa negara juga telah mengaturnya sebagai salah satu jenis kejahatan cyber (cybercrime). Penelitian ini akan membahas tentang e-mail spam di Indonesia, bagaimana peraturan perundang-undangan di Indonesia melihat perbuatan e-mail spam ini, apakah ada kemungkinan e-mail spam dikriminalisasi sebagai sebuah kejahatan cyber. Penelitian ini juga akan melihat bagaimana e-mail spam melanggar privasi dan mengkaji serta menganalisis pengaturan privasi internet di Indonesia dalam kaitannya dengan kriminalisasi e-mail spam tersebut.***Kata kunci*** *:* Kejahatan Siber, Forensik digital, keamanan web.

Kata Kunci: E-mail Spam, Media Cyber, Tindak Kejahatan.

Abstract

The Internet is part of the development of technology, where the internet provides many impacts, both positive and negative. Currently, privacy issues on the internet have also become a complicated legal issue, this is due to quite a number of privacy-related issues, but not all countries in the world manage privacy issues on the internet. As a means of communicating the Internet has introduced e-mail that provides convenience and practicality. But in its development e-mail has an adverse impact on its users in the form of e-mail spam. In terms of its actions, sending spam e-mail is quite a disadvantage, even violate the privacy. Some countries have also set it to one type of cybercrime (cybercrime). This research will discuss e-mail spam in Indonesia, how the legislation in Indonesia see the action of this spam e-mail, is there any possibility of spam e-mail is criminalized as a cybercrime. The research will also look at how spam e-mails violate privacy and review and analyze internet privacy settings in Indonesia in relation to the criminalization of spam e-mail.

Keywords: Spam E-mail, CyberMedia, Crime

PENDAHULUAN

Internet telah membawa dampak perubahan yang sangat besar bagi masyarakat. Dimana segala kegiatan manusia telah berganti menjadi aktivitas digital di dunia internet. Sebagai bagian dari konvergensi telematika, dimana terdapat tiga unsur yaitu telekomunikasi, media dan informatika, internet telah menjadi bagian tak terpisah- kan dalam kehidupan manusia.

Pemanfaatan e-mail sebagai kemudahan yang diberikan internet ini pun berpeluang ter- jadinya penyalahgunaan dimana dalam peng- gunaan e-mail dikenal pula e-mail spam. E-mail spam, merujuk pada definisi kata spam adalah email yang berisi konten "junk" (sampah) atau tidak re- levan dengan keperluan penggunanya (Anonim, 2015, www.techterms.com). Pengiriman e-mail spam dalam jumlah banyak, tentu menimbulkan ke- tidak nyamanan atau bahkan kerugian karena tak jarang konten dari e-mail spam tersebut berisi link- link yang mengarahkan penerima email untuk mengklik link-link tertentu yang berisi konten ber- bahaya.

Di Indonesia, e-mail spam juga menjadi masa- lah dalam penggunaan internet yang telah ada cukup lama. Bahkan pada tahun 2012, berdasarkan rilis data dari Kaspersky Lab, Indonesia termasuk pada peringkat ketujuh sebagai negara pengirim spam terbanyak dengan jumlah 3,1 persen (Riyandi Andesma, 2013, www.techno.okezone.com).

Internet merupakan dunia yang berbeda de- ngan dunia fisik yang kita kenal sehari- hari, ham- pir semua hal yang berhubungan dengan pelang- garan atau bahkan kejahatan tidak mampu disen- tuh oleh hukum positif yang berlaku di dunia fisik kita sehari-hari. Itulah mengapa dunia internet dan segala aktivitas yang terlibat di dalamnya dinama- kan dengan cyberspace dan aturan hukum yang meng- aturnya disebut cyberlaw.

Di Indonesia regulasi terkait cyberspace sen- diri telah diatur dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Dimana Undang-undang tersebut mengatur aspek-aspek hukum terkait internet baik perdata maupun pidana. UU ITE juga telah mengatur mengenai tindak pidana di internet dari Pasal 27 sampai Pasal 37, namun pengaturan mengenai penyebaran e- mail spam memang belum diatur secara spesifik. Beberapa tindak pidana dalam UU ITE antara lain baru mengatur mengenai pencemaran nama baik (Pasal 27 Ayat 3), penipuan konsumen (Pasal 28 Ayat 1), hacking (Pasal 30 Ayat 1) dan intersepsi (Pasal 32 Ayat 1).

Pemanfaatan teknologi informasi, media dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi telah pula menyebabkan hubungan dunia menjadi tanpa batas dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum [1]. Teknologi informasi yang semakin berkembang pesat dapat menjadi suatu ancaman ketika disalahgunakan seperti untuk aktivitas peretasan yang tentunya dapat merugikan. Manajemen keamanan sistem informasi dapat mengurangi terjadinya penyimpangan hak akses oleh pihak tertentu dan pernyalahgunaan data dan informasi sebuah organisasi atau perusahaan [2]

Ancaman keamanan terhadap sistem dan risiko serangan dapat berasal dari tiga aspek: integritas, kerahasiaan, dan ketersediaan[3]. Kejahatan siber atau yang dikenal dengan istilah cybercrime tentu menjadi suatu ancaman serius yang perlu diantisipasi dan ditangani dengan tepat, sebagai contoh dalam penerapan sistem informasi berbasis web tidak sedikit ditemukan kasus peretasan sehingga dari hal tersebut tentu perlu adanya suatu tindakan pengungkapan pelaku yaitu dengan dilakukannya forensik digital atau digital forensic yang merupakan suatu ilmu pengetahuan dan keahlian dalam melakukan identifikasi, analisa dan

pemetaan jaringan komunikasi pada suatu sistem informasi serta mengumpulkan bukti-bukti digital yang terkait dengan tindakan cybercrime tersebut. Beberapa teknologi tersebut antara lain deteksi spam, phishing deteksi, pemfilteran konten, dan pemfilteran lampiran [4]. Badan Siber dan Sandi Negara (BSSN) memprediksi peningkatan tren serangan siber, termasuk ransomware, kebocoran data, phising, dan social engineering pada tahun 2023 [5].

Banyaknya kasus peretasan data menjadi suatu ancaman dalam penerapan dan pemanfaatan suatu sistem informasi berbasis web [6]. Hal ini menjadi tantangan bagi Forensika teknologi informasi dan penegak hukum untuk melakukan penyelidikan terhadap barang bukti dari tersangka dalam kasus kejahatan karena bukti digital yang akan dijadikan sebagai barang telah dihapus oleh pelaku sehingga untuk mendapatkan kembali bukti digital, Forensika teknologi informasi dan penegak hukum dituntut untuk melakukan analisis forensik recovery data dalam mengembalikan data yang telah dihapus tersebut [7].

Digital forensik merupakan bagian ilmu forensik yang digunakan untuk penyelidikan dan penyidikan suatu perkara dalam investigasi materi (data) yang dan penemuan konten perangkat digital [8]. Sehingga dalam pengungkapan suatu kejahatan siber seperti peretasan situs web tersebut diperlukan adanya forensik digital yang bertujuan untuk mengidentifikasi, menganalisa dan memetakan jaringan komunikasi pada suatu sistem informasi berbasis web.

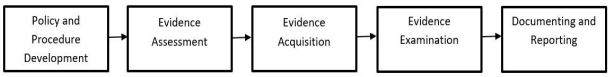
Adapun penelitian sebelumnya yang berjudul "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ)", penelitian ini membahas perbandingan terkait tool Forensik yang digunakan untuk proses eksaminasi dan analisa. Pengambilan salinan bukti digital dilakukan dengan metode forensik statik, sedangkan tahapan penelitian dan analisa mengadaptasi dan mengimplementasikan metode forensik dari National Institute of Justice (NIJ) untuk mendapatkan bukti digital. Software pembeku drive seperti Shadow Defender terbukti berpengaruh terhadap praktik eksaminasi forensik digital terhadap didapatkannya bukti-bukti digital, dengan kondisi tersebut prosentase keberhasilannya merestorasi file hanya 28,7% sehingga dapat menjadi hambatan dalam proses forensik digital [9].

Adapula penelitian dengan judul ""Investigasi Forensik Pada E-Mail Spoofing Menggunakan Metode Header Analysis", menjelaskan bahwa Email merupakan salah satu fasilitas internet yang banyak digunakan untuk komunikasi dan bertukar informasi. Hal ini memungkinkan pihak ketiga menyalahgunakan email untuk mendapatkan informasi secara ilegal dengan mengubah identitas pengirim email dan menjadikannya seperti email yang berasal dari email yang sah (legitimate email), aktivitas tersebut biasa dikenal dengan istilah email spoofing. Untuk dapat mendeteksi adanya email spoofing, maka perlu adanya investigasi forensik email terhadap email spoofing. Salah satu teknik investigasi forensik email adalah menggunakan analisis header email (header analysis method) [10].

Penelitian lainnya dengan judul "Perbandingan Kinerja Perangkat Lunak Forensik untuk File Carving dengan Metode NIST", penelitian ini melakukan perbandingan performansi perangkat lunak forensik open source untuk mengembalikan data, yaitu Scalpel, Foremost dan Autopsy, menggunakan metode forensik National Institute of Standards Technology (NIST). Proses pengujian yang dilakukan menggunakan teknik file carving. Hasil file carving dianalisis dengan melihat tingkat keberhasilan (akurasi) alat forensik yang digunakan dalam pengembalian data. Scalpel menunjukkan akurasi file carving tertinggi dengan keberhasilan sebesar 100% untuk 20 file dokumen dalam format pdf dan Docx, dan 90% untuk file gambar dalam format png dan jpeg [11].

Berdasarkan permasalahan diatas peneliti akan melakukan penelitian dengan judul Forensik Digital Sistem Informasi Berbasis Web Di Fakultas Teknik Universitas Muhammadiyah Sumatera Barat.

METODE



Gambar 1. Tahapan Forensik Digital

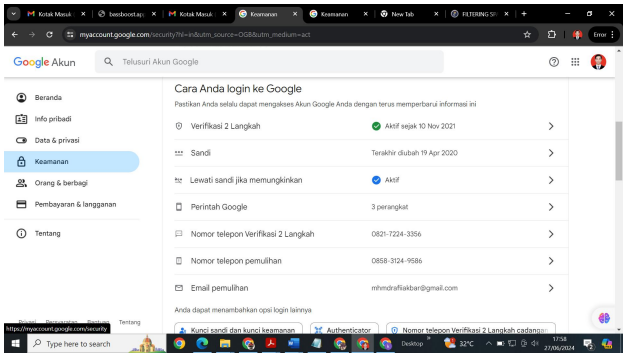
5 tahapan forensik digital tersebut masing-masing dapat dirinci berdasarkan pada studi kasus pada penelitian ini. Lebih jelasnya sebagai berikut :

1. *Policy and Procedure Development*.
   Memahami prosedur dan kebijakan pengembangan terkait dengan aturan atau regulasi pada objek yang akan dilakukan forensik digital, pada penelitian ini web yang digunakan sebagai objek forensik digital merupakan situs web yang dirancang khusus untuk keperluan simulasi pengujian.
2. *Evidence Assessment.*
   Penilaian barang bukti yang dapat berupa data, informasi rekam jejak, alur dan lain sebagainya yang terkait dengan konten digital sebagai barang bukti.
3. *Evidence Acquisition.*
   Pengumpulan barang bukti dari hasil penilaian barang bukti yang dianggap relevan sesuai dengan yang akan dilakukan forensik digital.
4. *Evidence Examination.*
   Pemeriksaan barang bukti dari hasil pengumpulan barang bukti.
5. *Documenting and Reporting.*
   Dokumentasi dan pelaporan dari hasil forensik digital.

HASIL DAN PEMBAHASAN

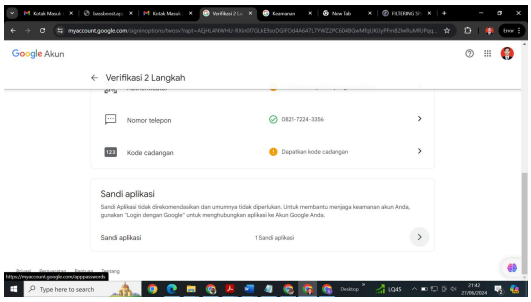
Pada penelitian ini, penelti menggunakan Scrip dari Python dengan mentarget objek/ email yang ingin di Boom dengan tujuan merusak email target yang telah banyak dimasuki spam dan bahasa email yang juga telah dibuat oleh pengirim sehingga pengguna email tersebut tidak mau lagi menggunakan email tersebut.

Langkah pertama yaitu buka terlebih dahulu email yang akan kita pakai untuk menyerang



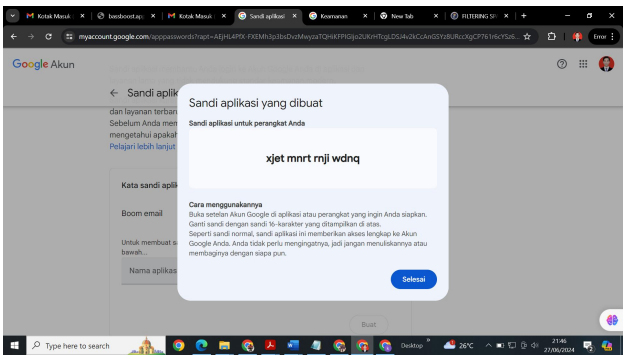
Gambar 2. Tampilan awal settingan email penyerang

Pada gambar 2 diatas dapat dilihat tampilan setinggan email si penyerang lalu lakukan settingan di keamanan dan aktifkan verivikasi dua langkah .



Gambar 3. Tampilan pemilihan sandi aplikasi

Pada gambar 3 diatas setelah pilih menu verifikasi dua langkah scrool kebawah terus pilih menu sandi aplikasi



Gambar 4. Sandi verifikasi supaya email bisa dipakai .

Pada gambar 4 diatas dapat dilihat merupakan sandi yang dibuat dari sandi aplikasi dan muncul kode-kode seperti digambar yang nantinya kode tersebut dimasukkan kedalam scrip phyton

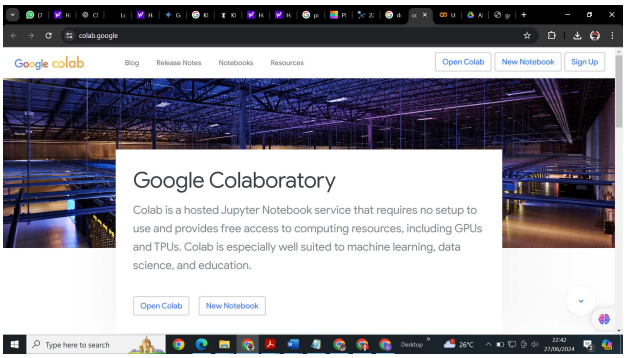
*Program Email Bomber - Notepad
File Edit Format View Help

```
import smtplib
toaddrs = 'halvcy@gmail.com'  (ini email target)
fromaddrs = 'xyzrafiakbar@gmail.com' (Email Pengirim)

message = 'Hallo Salam Kenal' (pesan yang mau dikirimkan)
with smtplib.SMTP('smtp.gmail.com', '587') as smtpserver:
  smtpserver.ehlo()
  smtpserver.starttls()
  smtpserver.ehlo()
  smtpserver.login('xyzrafiakbar@gmail.com','axotazpvxatpsmyh')
  for i in range(5): (berapa jumlah emai yang mau di Boom)
    smtpserver.sendmail(fromaddrs, toaddrs, message)
    print(i)
```

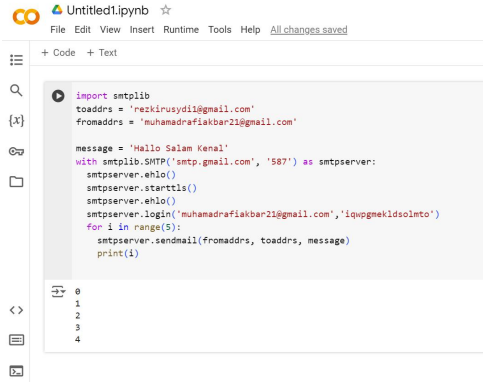
Gambar 5. Scriping python untuk boom mail.

Pada gambar 5 diatas sudah kami jelaskan pada toaddrs yang kita masufromaddrs disitu kita masukkan email penyerang yang telah tervervikasi dua langkah dan telah muncul menu sandi aplikasinya, untuk smtpserver login disitu masukkan email penyerang dan sandi yang telah dibuat pada email penyerang sebelumnya



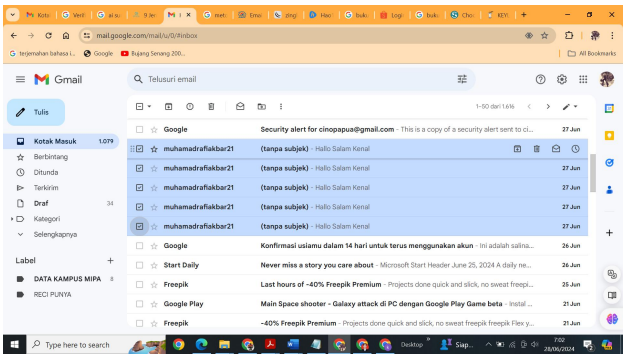
Gambar 6. Tampilan awal Google Colab

Pada gambar 6 diatas dapat Google Colab sendiri diperuntukkan dengan mempertimbangkan kebutuhan machine learning programmers, big data analysts, data scientists, AI researchers, and Python learners.



Gambar 7. Hal Sript Coding Boom Mail

Pada gambar 7 diatas bahwasanya telah di inputkan coding untuk boom mail yang mana target emailnya disana adalah email rezkirusydi1@gmail.com dan di boom sebanyak lima kali perulangan



Gambar 8. Hasil gambar email yang terkena boom

Pada gambar 8 diatas telah ditampilkan di email yang diserang sudah masuk email yang tidak terduga dengan jumlah perulangan lima kali dan bahwasanya itu telah menjelaskan bahwa penyerang berhasil melakukan boom mail terhadap terget.

KESIMPULAN

Berdasarkan hasil dan pembahasan, maka didapatkan kesimpulan bahwa aplikasi Maltego dapat digunakan untuk keperluan forensik digital pada suatu situs web dalam upaya mengumpulkan informasi dan memetakan jaringan komunikasi apa saja yang terkait didalamnya dengan melakukan pelacakan domain utama, situs yang masih terikat pada domain tersebut yang ditampilkan pada Maltego.

Hasil penelitian ini dapat digunakan sebegai solusi dalam menangani sebuah kasus yang membutuhkan barang bukti digital. Informasi ini dapat divisualisasikan dalam bentuk pemetaan jaringan komunikasi dan informasi yang mudah dipahami.

DAFTAR PUSTAKA

Riskawati, Riskawati; Tahir, H. (2016). PENANGANAN KASUS CYBER CRIME DI KOTA MAKASSAR (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). Jurnal Tomalebbi, 2, 93–103.

Adiyono, Soni, dkk. (2022). FRAMEWORK MANAGEMENT TO MINIMIZE RISK IN PROTECTING ENTERPRISE SYSTEMS: SYSTEMATIC LITERATURE REVIEW. Telematika: Jurnal Informatika dan Teknologi Informasi. Vol. 19, No. 2, Juni 2022, pp.159-172.

Pratama, Tino Imam Maulana, Songida, Gunawan. 2022. Analisis Serangan dan Keamanan pada SQL Injection: Sebuah Review Sistematik. JIIFKOM (Jurnal Ilmiah Informatika & Komputer) STTR Cepu. Hal.28.

Altulaihan, Esra, dkk. 2023. Email Security Issues, Tools, and Techniques Used in Investigation. Sustainability.

Putri, Nur Dwi, Dahliyusmanto. 2024. Analisis Keamanan Menggunakan Metode Live Forensic pada Web. Jurnal Teknlogi Informatika dan Komputer MH. Thamrin. Volume 10 No 1.

Andria;Ningrum, W. A., & Mubarok, I. (2021). PENGUJIAN KEAMANAN BASIS DATA SISTEM INFORMASI BERBASIS WEB. PROSIDING SNAST, 66–74.

Riadi, I., Sunardi, S., & Sahiruddin, S. (2019). Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ). Jurnal Rekayasa Teknologi Informasi (JURTI), 3(1), 87–95

Rachmie, S. (2020). PERANAN ILMU DIGITAL FORENSIK TERHADAP PENYIDIKAN KASUS PERETASAN WEBSITE. JURNAL LITIGASI (e-Journal), 21(1), 104–127

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij). Evo (Electronics, Informatics, and Vocational Education), 3(1), 70–82

Hoiriyah, H., Sugiantoro, B., & Prayudi, Y. (2016). Investigasi Forensik pada E-mail Spoofing menggunakan Metode Header Analysis. Data Manajemen Dan Teknologi Informasi,17(4), 20–25.

Yuwono, D. T., Fadlil, A., & Sunardi, S. (2019). Perbandingan Kinerja Perangkat Lunak Forensik untuk File Carving dengan Metode NIST. Jurnal Teknologi Dan Sistem Komputer, 7(3), 89–92

Andria, Sekreningsih Nita. 2021. FORENSIK DIGITAL SISTEM INFORMASI BERBASIS WEB. JURNAL AHLI MUDA INDONESIA. Vol. 2 No. 2. Hal. 142.