

# Analisis Ancaman *Phishing* Di Platform Media Sosial Email menggunakan Metode *Digital Forensic Research* Workshop

*Analyzing phishing threats in email social media platforms using digital forensic research workshop methods*

**Shofiyyah Nailah<sup>a,1</sup>, Rika Rosnelly<sup>b,2</sup>**

<sup>a</sup>Universitas Potensi Utama, KL. Yos Sudarso, Medan, 20241, Indonesia

<sup>b</sup> <sup>a</sup>Universitas Potensi Utama, KL. Yos Sudarso, Medan, 20241, Indonesia  
shofiyyah.nailah21@gmail.com<sup>1</sup>, rikarosnelly@gmail.com<sup>2</sup>

---

## ABSTRAK

Metode digital forensic research workshop digunakan dalam penelitian ini untuk menganalisis resiko phishing di platform media sosial dan email. Tujuan utama dari penelitian ini adalah untuk mengidentifikasi teknik phishing yang digunakan dan menguji apakah halaman media sosial dapat dikloning untuk mencuri data pengguna saat mereka log in. phishing adalah spoofing sebagai cara untuk menyebarkan tautan phishing juga dibahas dalam penelitian ini. Penelitian ini menggunakan DFRWS dikarenakan setiap langkah yang diambil dapat memberikan penjelasan menyeluruh tentang tahapan forensic ini yang mencakup identifikasi, perlindungan, pengumpulan, pemeriksaan, analisis dan presentasi adalah untuk membantu mendapatkan bukti dan mekanisme untuk merekam data yang dikumpulkan.

Metode digital forensic research workshop digunakan dalam penelitian ini untuk menganalisis resiko phishing di platform media sosial dan email. Tujuan utama dari penelitian ini adalah untuk mengidentifikasi teknik phishing yang digunakan dan menguji apakah halaman media sosial dapat dikloning untuk mencuri data pengguna saat mereka log in. phishing adalah spoofing sebagai cara untuk menyebarkan tautan phishing juga dibahas dalam penelitian ini. Penelitian ini menggunakan DFRWS dikarenakan setiap langkah yang diambil dapat memberikan penjelasan menyeluruh tentang tahapan forensic ini yang mencakup identifikasi, perlindungan, pengumpulan, pemeriksaan, analisis dan presentasi adalah untuk membantu mendapatkan bukti dan mekanisme untuk merekam data yang dikumpulkan. Edukasi phishing akan sangat membantu masyarakat untuk berjaga-jaga akan media sosial yang sedang digunakan setiap harinya. Untuk meningkatkan kewaspadaan pada semua media sosial yang digunakan termasuk pada media sosial platform email, meski tidak sering digunakan tetapi email menjadi titik tumpu untuk masuk pada semua akun sosial media. Untuk membangun kewaspadaan pada semua kalangan masyarakat agar tidak mudah mempercayai link yang disebarluaskan dengan alasan khusus.

---

Kata Kunci : DFRWS, Phishing, Spoofing

## ABSTRACT

The digital forensic research workshop method was used in this study to analyze the risk of phishing on social media platforms and email. The main objective of this research is to identify the phishing techniques used and test whether social media pages can be cloned to steal user data when they log in. phishing is spoofing as a way to spread phishing links is also discussed in this research. This research uses DFRWS because each step taken can provide a thorough explanation of these forensic stages which include identification, protection, collection, examination, analysis and presentation is to help obtain evidence and mechanisms to record the data collected. Phishing education will greatly help the public to be aware of the social media that is being used every day. To increase vigilance on all social media used including on social media email platforms, although not often used but email is the fulcrum for logging into all social media accounts. To build awareness in all circles of society so as not to easily trust the links that are spread for special reasons.

Keywords : DFRWS, Phishing, Spoofing

---

Disubmit: 11 Januari 2025

Info Artikel :  
Direview: 15 Februari 2025

Diterima : 12 Maret 2025

---

Copyright © 2025 - Journal UPU. All rights reserved.

---

DOI: <https://www.doi.org/10.22303/upu.1.1.2021.01-10>

## 1. PENDAHULUAN

*Phishing* adalah Cara Mendapatkan Informasi (Nama Pengguna, Kata Sandi, Informasi Kartu Kredit), *Phishing* adalah metode penipuan yang dapat dirilis saat Anda menggunakan ID imitasi untuk mendapatkan informasi dari selesai. Dalam sistem administrator, sebagian besar bertanggung jawab atas keselamatan sistem mereka sendiri, yang sebagian besar tidak memiliki jaringan penting di dunia luar. Sistem pengujian untuk memastikan efisiensi dan akurasi pemrosesan data sangat mahal saat ini.

Memancing adalah jenis kegiatan di mana konsep pemancing ini melibatkan mengancam atau menangkap seseorang. Yaitu, melalui seseorang yang menipu sedemikian rupa sehingga seseorang secara tidak langsung memberikan semua informasi yang mereka butuhkan untuk menjebak. *Phishing* termasuk dalam kejahatan dunia maya [1]. Saat ini ada sejumlah tindakan kriminal yang terkait dengan jaringan komputer. Seiring waktu, kegiatan kriminal menjadi semakin luas di seluruh dunia. Dengan demikian, banyak ancaman muncul dari komputer saat ini [2]. Media sosial adalah tempat di mana orang dapat berhubungan dengan keterpencilan dan di mana informasi dapat diakses dengan cepat [3]. Hampir semua orang di dunia menggunakan media sosial. Ini berarti bahwa aktivitas kejahatan dunia maya menggunakan peluang untuk menerapkan langkah-langkah terhadap pengguna media sosial.

*Digital Forensic Research Workshop* adalah salah satu metode *Digital forensic* yang sering digunakan untuk menganalisis masalah kejahatan yang sangat sering terjadi pada dunia digital[4]. Banyak keuntungan dalam menganalisis kasus digital dengan menggunakan metode DFRWS. Pada umumnya banyak sekali metode yang digunakan untuk menganalisis suatu kasus *forensic* tetapi jika kita tidak menggunakan metode DFRWS dalam penyelidikan kasus Digital maka akan ada beberapa problem yang dapat terjadi pada penyelidikan kasus, beberapa hal yang dapat disebutkan adalah kehilangan bukti digital, biasanya tanpa DFRWS bukti-bukti digital yang penting dalam penyelidikan kejahatan *cyber* dapat terabaikan[5].

Metode *Digital Forensic Research Workshop* (DFRWS) ini memberikan bukti mekanisme untuk merekam segala informasi yang dibutuhkan[6]. Hasil dari penelitian menggunakan metode ini adalah pencarian bukti pada kejahatan digital lebih mudah ditemukan ketika menggunakan metode DFRWS karena dapat menemukan bukti dengan sangat teliti dan merekam segala jejak dan informasi untuk penyelidikan, *Digital Forensic Research Workshop*[6] digunakan untuk menyelesaikan penyelidikan kejahatan pada digital, dengan menggunakan metode ini keuntungan dalam pencarian lebih tepat, seperti pemodelan proses investigasi metode ini menyediakan kerangka kerja yang sistematis untuk menyelidiki kejahatan digital, mulai dari identifikasi masalah hingga presentasi hasil penyelidikan.

Berdasarkan hal tersebut saya sebagai penulis mengambil judul“ ANALISIS ANCAMAN *PHISHING* DI PLATFORM MEDIA SOSIAL EMAIL MENGGUNAKAN METODE *DIGITAL FORENSIC RESEARCH WORKSHOP* (DFRWS)”.

### A. Permasalahan Penelitian

- 1) Semakin meningkatnya serangan *phishing* dari waktu ke waktu. Hal ini membuat semakin banyak masyarakat yang menjadi korban serangan tersebut.
- 2) Banyaknya pengguna internet yang kurang memahami serangan *phishing* dan ingatkanbagaimana cara mengidentifikasinya. Hal itu meningkatkan mereka rentan menjadi korban serangan *phishing*.
- 3) Teknologi yang semakin berkembang membuat para penyerang *phishing* terus mengembangkan teknik-teknik baru untuk mengelabui korban dan menghindari deteksi oleh sistem.

### B. Tujuan penelitian

- 1) Menganalisis dan mengidentifikasi serangan *phishing* dan karakteristiknya
- 2) Meneliti pengembangan teknik *phishing* terbaru dengan berfokus pada teknik-teknik yang masih relevan.
- 3) Menganalisis modus operasi *phishing* di platform email, faktor yang menyebabkan kerentanan pengguna, dan strategi pencegahan *phishing* yang efektif.

### C. Manfaat penelitian

- 1) Meningkatkan kesadaran masyarakat tentang bahayanya serangan phishing serta cara mengidentifikasi serangan ini.
- 2) Berpotensi untuk menjadi sumber pengetahuan yang berguna bagi penelitian dan pihak-pihak terkait dalam upaya melindungi masyarakat dari serangan phishing.
- 3) Menjadi bahan kajian dan analisis penting untuk perlindungan data pribadi serta pertanggung jawaban pelaku kejahatan phishing.

## 2. METODE

Untuk mendapatkan data-data yang mendukung didalam penelitian ini, maka penulis menggunakan metode, yaitu:

### A. Metode Lapangan

Merupakan metode yang dilakukan dengan mengadakan langsung ke lapangan untuk mengumpulkan data yaitu peninjauan langsung ke lokasi studi. Adapun teknik pengumpulan data yang dilakukan penulis adalah:

- a. *Studi Dokumentasi*  
Studi dokumentasi merujuk pada teknik pengumpulan data yang dilakukan dengan mengumpulkan dan menganalisis dokumen-dokumen.
- b. *Wawancara*  
Pengumpulan data atau informasi pada metode ini dapat dilakukan dengan wawancara atau mengajukan pertanyaan-pertanyaan langsung pada masyarakat dalam permasalahan pengguna setelah terkena link phishing
- c. *Kuisisioner*  
Kuisisioner merupakan serangkaian pertanyaan tertulis yang disusun secara sistematis untuk mengumpulkan informasi dari responden.

### B. Bahan penelitian

Adapun bahan penelitian yang dapat menyempurnakan penelitian ini yaitu:

- 1) Jenis Bahan phishing
  - a. phishing classic: Penyerang menggunakan email yang menarik atau pesan SMS untuk membuat korban tersedia untuk memberikan informasi pribadi.
  - b. spear phishing: Penyerang bertujuan untuk menggunakan orang-orang tertentu dengan menggunakan informasi pribadi yang dikumpulkan sebelumnya untuk membuat pesan yang tampak valid.
  - c. whaling: Bentuk spearphish terus menerus yang bertujuan menargetkan individu dengan posisi tinggi atau asli dalam bentuk jaringan.
  - d. pharming: Penyerang mengarahkan korban ke situs web palsu dengan memanipulasi sistem DNS atau menggunakan malware untuk menggunakan alamat IP yang diterima oleh ZZ [7].
- 2) Metode penyerangan phishing:
  - a. Penyerang mengirimkan email yang tampak asli, sering kali dengan tautan atau lampiran yang mengarah ke situs web palsu yang meniru institusi atau layanan yang dikenal oleh korban.
  - b. Phishing melalui SMS (Smishing): Penyerang mengirimkan pesan teks yang berisi tautan atau instruksi untuk mengungkapkan informasi pribadi.
  - c. Phishing melalui Telepon (Vishing): Penyerang menggunakan panggilan telepon untuk mendapatkan informasi sensitif dari korban dengan berpura-pura menjadi entitas tepercaya.
  - d. Phishing melalui Situs web Palsu: Penyerang menciptakan situs web palsu yang meniru tampilan dan nuansa situs resmi untuk meminta pengguna memasukkan informasi pribadi mereka.

e. Jenis serangan pada phishing sangat banyak caranya, berikut adalah laporan insiden yang sering terjadi pada Indonesia:

a) Phishing berkedok aplikasi email

Cara ini biasanya target mengirimkan link palsu untuk melakukan perubahan data data perbankan, cara ini sudah lama dilakukan perera tindak criminal dalam melakukan pencurian data data nasabah Bank. Target melakukan *Phishing* dengan cara Spam *Email* dengan keterangan palsu seperti : Info *Login* dan *Password*, Info Perubahan data Nasabah. Jika Nasabah tersebut tidak teliti maka nasabah akan mengklik link yang diberikan pelaku dan nasabah akan menginput data data ke dalam link palsu yang diberikan Pelaku[8].

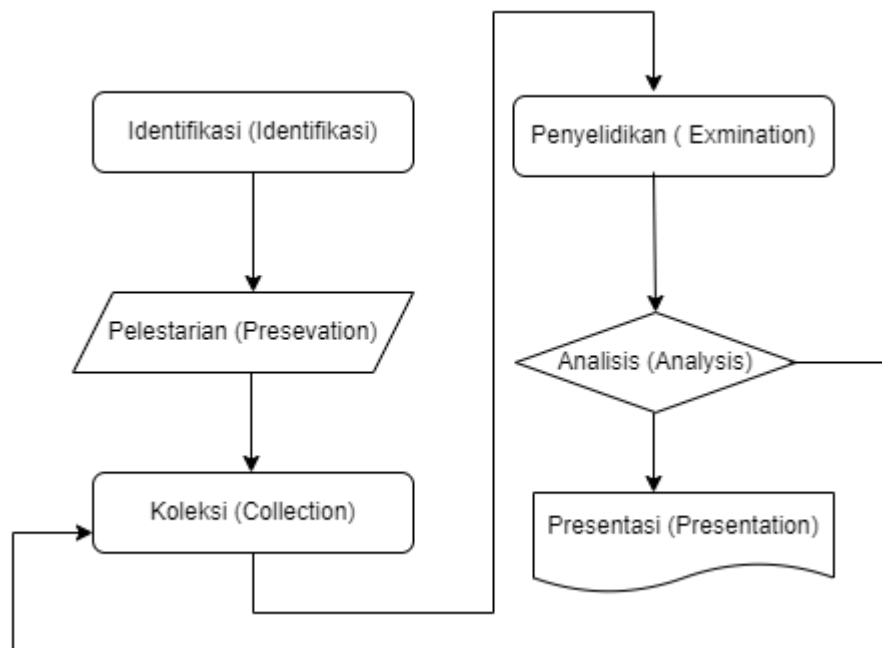
3) Langkah-langkah Melindungi Diri dari Phishing

Langkah-langkah yang harus dilakukan untuk melindungi diri dari serangan phishing adalah sebagai berikut[9]:

- Selalu periksa URL. Pastikan situs web yang Anda kunjungi menggunakan protokol "https" dan memiliki sertifikat keamanan yang valid.
- Jaga Kerahasiaan Informasi Pribadi: Hindari memberikan informasi sensitif melalui email, pesan teks, atau panggilan telepon yang tidak dapat dipercaya.
- Waspada Tautan dan Lampiran: Jangan mengklik tautan atau membuka lampiran dari sumber yang tidak dikenal atau mencurigakan.
- Gunakan Antivirus dan Perangkat Lunak Keamanan: Selalu perbarui perangkat lunak keamanan Anda dan gunakan firewall serta program antivirus yang andal.
- Tingkatkan Kesadaran Keamanan: Edukasi diri sendiri dan orang lain tentang taktik phishing yang umum digunakan serta tanda-tanda peringatan yang perlu diwaspadai[10].

C. Metodologi Penelitian

Metode penelitian merupakan alur atau langkah-langkah dalam penyusunan penulis, berikut akan digambarkan melalui flowchart mulai dari proses perencanaan hingga pembuatan dokumentasi. Penelitian yang dilakukan dengan menggunakan metode forensic digital yang dikembangkan oleh *Digital Forensic Investigation Workshop* (DFRWS). Alur metodologi dalam tugas akhir ini dapat dilihat pada Gambar III.1[3]:



Gambar 1. Alur Proses DRWRS

- 1) Identifikasi ( Identification)  
Tahap ini dilakukan untuk menentukan apa yang diperlukan untuk melakukan penyelidikan dan pencarian bukti kasus yang akan diproses. Proses ini menentukan kebutuhan yang dibutuhkan selama ujian dan mencari bukti dari tim ujian. B. Mengamankan bukti fisik dalam bentuk smartphone untuk para korban.
- 2) Pemeliharaan (preservation)  
Fase ini dilakukan untuk melindungi bukti yang disimpan untuk perlindungan bukti digital, memastikan kredibilitas bukti, dan untuk melawan klaim bahwa bukti itu palsu. Dalam proses ini, peneliti mempertahankan dan menyimpan bukti digital dan memastikan kredibilitas bukti. Internet.
- 3) Koleksi (collection)  
Anda dapat menyelesaikan proses mengumpulkan dan mengidentifikasi file atau data dari bukti dan memasukkannya sebagai sumber data. Proses ini melibatkan pengumpulan bukti digital melalui alat forensik yang dilakukan oleh peneliti.
- 4) Penyelidikan (examination)  
Keandalan data penting dengan menentukan langkah -langkah untuk menentukan pemilihan data untuk beberapa sumber data tertentu, sehingga pemilihan data dilakukan dengan menerima formulir data tanpa memodifikasi konten data. Sebagai hasil dari pengumpulan data. Filter data dijalankan untuk mengurutkan data dan membatasi data ke bagian tertentu dari sumber data yang dijalankan. Ini berisi folder dan file untuk menemukan data yang dijalankan dalam proses analisis, seperti folder basis data yang diekstraksi dengan alat forensik. 1 Contoh data Pro 1 dapat ditemukan di folder Chace.
- 5) Analisis (analysis)  
Tentukan di mana data dihasilkan, siapa yang bisa melakukannya, bagaimana itu dilakukan, dan mengapa itu dibuat. Proses ini menentukan di mana data tersedia, di mana ia datang dan jenis data apa itu. Ini untuk mengejar evaluasi bukti dan bukti, seperti B. Tag video yang dihapus oleh pelaku kejahatan. Lacak dan temukan hasil yang diekstraksi sebelumnya dalam folder database/chaquer/jawaban/profile\_feed.
- 6) Presentasi (presentation)  
Presentasi dilakukan dengan menyajikan informasi yang dibuat selama fase analisis. Tingkat presentasi diambil dari proses ujian setelah proses inspeksi dianalisis. Selain itu, fase ini menjelaskan alat dan metode yang digunakan, menentukan prosedur yang didukung yang diterapkan, dan memberikan rekomendasi untuk meningkatkan pedoman atau pesanan, metode, alat, atau aspek pendukung lainnya. Fase akhir dari metode DFRWS membuat laporan terperinci tentang laporan dengan membuat tabel laporan tentang jumlah bukti yang ditemukan.

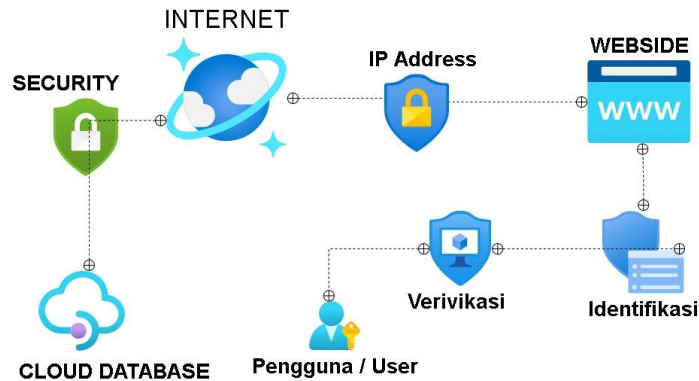
### 3. HASIL DAN PEMBAHASAN

#### A. Pengembangan Source Code

Source code merupakan bahasa pemrograman untuk membuat sebuah Aplikasi dan webside, source code juga ada beberapa jenis seperti[11] :

1. HTML
2. JAVA
3. PHP
4. Python

Keempat Bahasa Pemograman tersebut bias menghasilkan aplikasi seperti Apk *Smatphone* dan *WebSide*. Jika Dikembangkan secara *Expert* dan saling terintegrasi akan menghasilkan suatu pola yang saling Terhubung , hal seperti ini di sebut ERP ( *Enterprise Resourc Planning* ). Sumber berasal dari ([www.google.jaringan\\_website.com](http://www.google.jaringan_website.com))

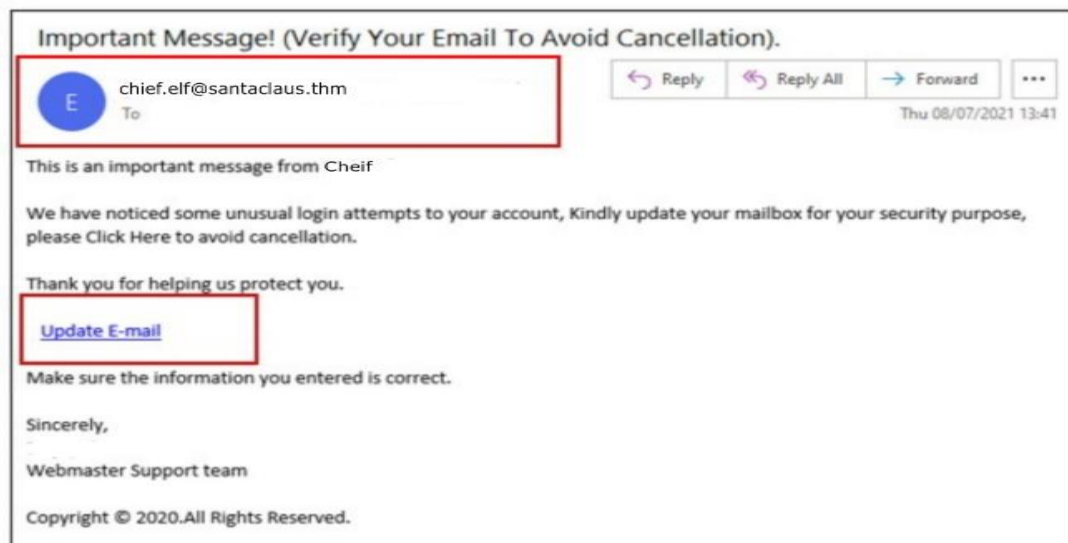


Gambar 2. ilustrasi jaringan *website*

Dari gambar diatas , kita ketahui *security*, identifikasi dan verifikasi merupakan benteng pertahanan sebagai *security*. Hal inilah membuat para pelaku *cyber* termasuk *Phising* untuk mencari celah untuk mempengaruhi ke lalaian pengguna.

a. Identifikasi *Phishing*

Identifikasi merupakan salah satu tahapan terpenting dalam DFRWS yang bertujuan untuk menemukan dan mendokumentasikan bukti digital yang relevan dengan suatu kasus. Awal mula 1980-1990 pada masa ini focus utama identifikasi *digital forensic* adalah pada penemuan media penyimpanan fisik, seperti *hard disk drive*, *floppy disk* dan CD-ROM. Pada tahun 2000 perkembangan teknologi *digital forensic* mendorong pengembangan alat dan teknik baru untuk identifikasi bukti digital. Pada tahun 2010-sekarang seiring dengan semakin kompleks kasus-kasus *digital forensic*, pendekatan holistik menjadi lebih penting dalam proses identifikasi[12].



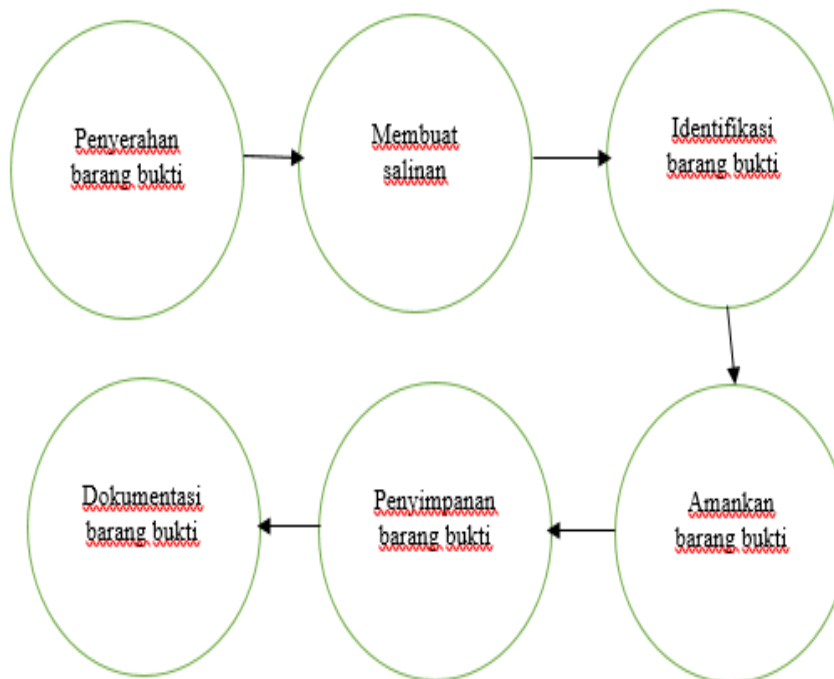
Gambar 3. *Phishing melalui email*

Gambar diatas adalah cara pelaku memanipulasi data informasi yang di kirim melalui *email* dengan menggunakan instansi terkenal untuk memancing korban agar dapat mengklik link yang sudah dikirim. Ketika Korban Mengklik salah satu link makan korban akan masuk ke *webside* yang sudah di manipulasi *sourcecode* dan korban akan mengklik update pada *website* tersebut, nah di sinilah data

pribadi korban berupa *username*, *password* atau lainnya akan masuk di sistem pelaku. Cara ini pernah tren di tahun 2009 – 2012 yang digunakan para *Cracker Spam Phising*. Disaat *Smartphone* sudah ada dan banyak diminati masyarakat maka pengembangan *source code* juga terus update oleh perkembangan teknologi nya. masyarakat dimanja dengan teknologi mulai dari Belanja *Online*, Pembayaran *online*[13]. Hal ini juga jadi tantangan para *Cyber crime Spamming* dengan pengembangan Dengan Cara *Phising*[14].

b. Pelestarian

Pelestarian adalah salah satu tahap terpenting dalam *Digital Forensic Research Workshop* (DFRWS) yang bertujuan untuk memastikan bahwa bukti digital tidak diubah atau dirusak selama proses investigasi. Proses ini dilakukan untuk menyimpan barang bukti digital agar tidak berubah dan terganggu. Pelestarian bukti digital penting untuk menjaga integritas dan penerimaan bukti di pengadilan. Berikut adalah beberapa hal yang perlu diperhatikan dalam pelestarian bukti digital



Gambar 4. urutan pelestarian barang bukti

- 1) Memebuat Salinan dari perangkat penyimpanan data yang releven
- 2) Mengidentifikasi data tersembunyi untuk memastikan semua data yang tersembunyi teridentifikasi dan dipulihkan. Bukti digital yang telavan diidentifikasi dan dicatat. Ini mencakup penentuan lokasi perangkat dan jenis data yang ada.
- 3) Pengamanan, setelah diidentifikasi langkah selanjutnya adalah mengamankan data tersebut. Ini melibatkan pembuatan Salinan dari data asli menggunakan teknik yang tidak merusak, seperti hashing untuk memastikan bahwa Salinan tersebut identic dengan aslinya.
- 4) Penyimpanan, setiap bukti digital harus disimpan dalam lingkungan yang aman dan steril untuk mencegah perubahan atau kerusakan. Penyimpanan ini harus dilakukan dengan prosedur yang ketat untuk menjaga integritas data.
- 5) Dokumentasi, setiap langkah dalam proses pelestarian harus didokumentasikan secara rinci. Ini termasuk pencatatan waktu, metode yang digunakan, dan siapa yang melakukan setiap tindakan. Dokumentasi ini penting untuk membuktikan bahwa prosedur yang benar telah diikuti.

## c. Koleksi

Koleksi merupakan salah satu tahap penting dalam *Digital Forensic Research Workshop* yang bertujuan mengumpulkan bukti digital dari perangkat atau media penyimpanan dengan cara *forensic* yang benar. Barang bukti yang dapat di koleksi untuk menyidikan adalah link yang diterima oleh korban yang dikirim oleh para *cyber crime* yang ingin mencuri data, berikut contoh link:

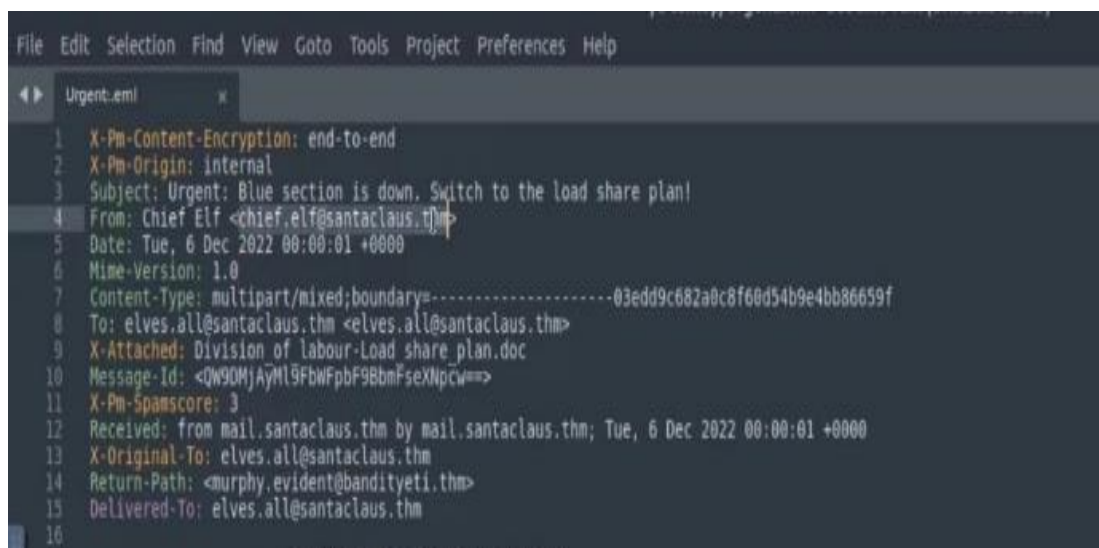


Gambar 5. Link phishing

Berikut adalah contoh phishing yang di terima oleh korban dengan mengiming-imingkan untuk melihat pesanan yang di kirim pada pihak instansi tertentu agar korban dapat mengklik link yang sudah mereka buat untuk menjebak para korban agar mendapatkan data diri korban.

## d. Penyelidikan

Dengan melakukan langkah penentuan seleksi data pada bagian-bagian dari beberapa sumber data tertentu, seleksi data dilakukan dengan mengasumsikan bentuk dari data, tetapi tanpa mengubah isi data karena keaslian data itu sangatlah penting dalam penyelidikan.



Gambar 6. Tampilan isi pada link

Pada gambar yang ditampilkan diatas adalah tahap awal dari pemecahan link disebar, penggunaannya menggunakan *sublime text* yang dilakukan di *linux* untuk mendeteksi source pada *phishing* yang dikirim.



Gambar 7. menampilkan data penyelidikan

Gambar diatas adalah gambar yang harus diisi untuk menampilkan penyelidikan yang di lakukan pada pembedahan link yang menampilkan hasil coding. Pada gambar ini akan menampilkan email yang ada dalam coding bedah pada link, email pelaku ada pada gambar IV.4 pada baris ke 4, yaitu [chief.elf@santaclaus.thm](mailto:chief.elf@santaclaus.thm).



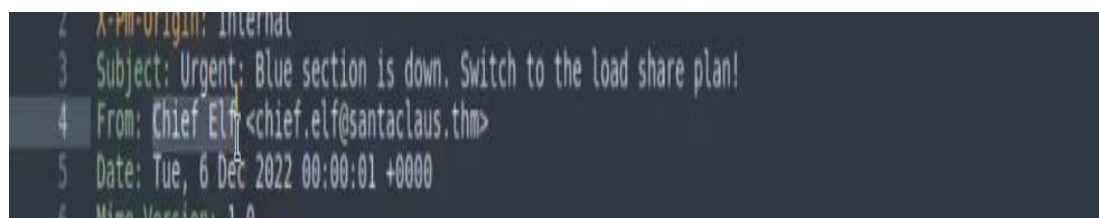
Gambar 8. tampilan pada isi link

Tahap ini adalah alamat pada pengirim untuk menerima data diri yang masuk, terdapat pada line ke-14 dimana *return-path* menunjukkan alamat yang akan menerima data diri korban akan masuk ke [murphy.evident@bandityeti.thm](mailto:murphy.evident@bandityeti.thm). Pelaku *cyber* melakukan *spoofing* pada *email*, Ketika korban membalas *email*/mengklik yang ada pada email data akan masuk ke [murphy.evident@bandityeti.thm](mailto:murphy.evident@bandityeti.thm) bukan masuk ke alamat email [chief.elf@santaclaus.thm](mailto:chief.elf@santaclaus.thm).



Gambar 9. melengkapi data penyelidikan

setelah diketahui alamat pada email yang akan menerima data diri korban yang sudah di perlihatkan pada gambar IV.7 yaitu [murphy.evident@bandityeti.thm](mailto:murphy.evident@bandityeti.thm) lalu akan di proses untuk melengkapi data-data yang harus dicari untuk melengkapi data pengirim. Murphy adalah nama asli dari pelaku dan menyamarkan nama menggunakan chief elf untuk mengirim kan pesan tersebut.



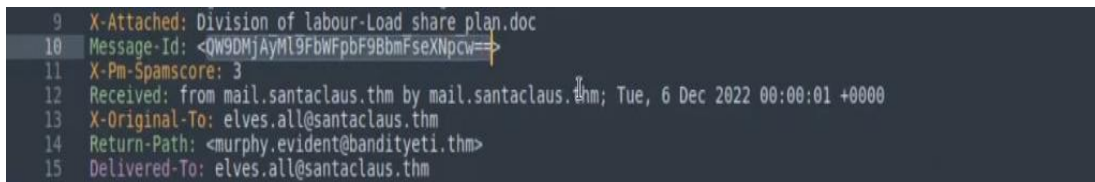
Gambar 10. Pencarian Nama Pengirim

Pada tahap ini pembongkaran yang menggunakan *sublime* pada *linux* dapat mencari tau pengiriman *phishing* ini mengatasnamakan siapa. Terdapat pada line ke-4 dimana *form* ini adalah nama pelaku yang sudah melakukan spoofing untuk menyamarkan identitasnya.

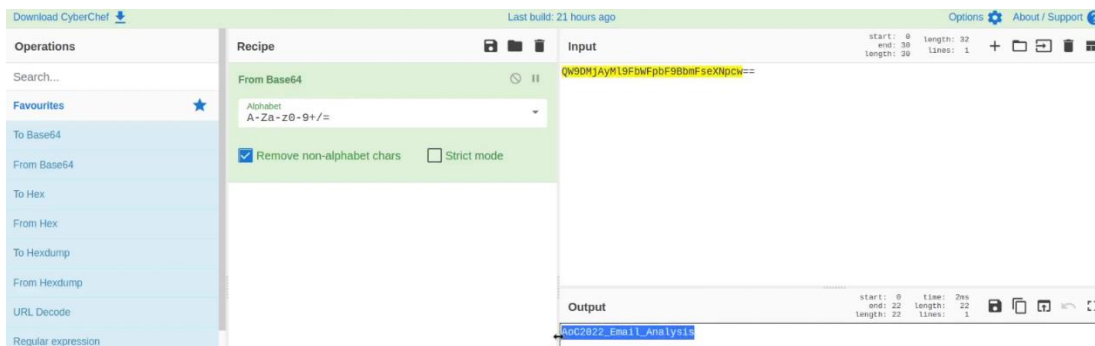


Gambar 11. Melengkapi Data Penyelidikan

Pada tahap ini untuk melengkapi data penyelidikan akan dimasukan nama yang terbaca oleh penerima *phishing*.

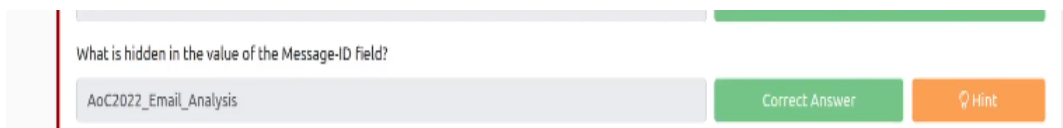
Gambar 12. Nilai Tersembunyi Pada *Phishing*

Pada tahap ini nilai tersembunyi yang ada pada *phishing* adalah kata-kata yang ter *en-coding* dengan base 64. Dengan ini penulis menggunakan tools lain untuk melihat nilai yang tersembunyi pada *phishing* sebelum dimasukkan kedalam *tools cyberchef* untuk melakukan penyelidikan yang akan dilengkapi.



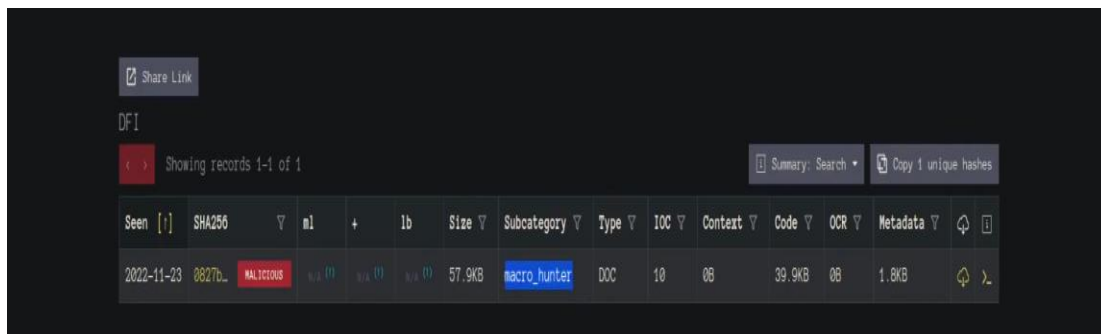
Gambar 13. Mencari Nilai Tersembunyi

Pada tahap ini penyelidikan yang dilakukan menggunakan *tools cyberchef* untuk mencari nilai tersembunyi yang ter *en-coding*. Nilai sebelumnya adalah `<QW9DMjAyMl9FbWp9BbMFseXNpcw==>`, setelah dilakukan pencarian nilai maka hasil dari yang dilakukan adalah `AoC2022_Email_Analysis`.



Gambar 14. Melengkapi Data Penyelidikan.

Untuk melengkapi pendataan agar dapat melihat hasil pada virus apa yang terdapat pada *phishing* setelah melakukan beberapa pembongkaran dan mengisi pendataan dengan beberapa *tools* untuk dilakukannya penyerahan data.



| Seen       | SHA256   | ml        | lb | Size   | Subcategory  | Type | IOC | Context | Code   | OCR | Metadata |  |
|------------|----------|-----------|----|--------|--------------|------|-----|---------|--------|-----|----------|--|
| 2022-11-23 | 0827b... | MALICIOUS |    | 57.9KB | macro_hunter | DOC  | 10  | 06      | 39.9KB | 06  | 1.8KB    |  |

Gambar 15. Hasil

Pada tahap ini adalah hasil dari penyelidikan yang menampakan bentuk *type*, *size file*, dan *subcategory* pada file phishing tersebut. Pada file ini menunjukkan bahwa *subcategory* nya adalah *macro\_hunter* yang berarti file ini *malware* yang berbahaya.

e. Analisis

Analisis merupakan salah satu tahap penting yang bertujuan untuk menemukan dan menginterpretasikan informasi yang relevan dari bukti digital yang dikumpulkan[14]. Analisis yang dilakukan adalah analisis bukti yang sudah terjadi dan berapa persen hal ini sering terjadi dan kalangan mana saja yang rentan terkena penipuan *phishing* tersebut[15].

f. Presentasi

Presentasi merupakan salah satu tahap penting yang bertujuan untuk mengkomunikasikan hasil investigasi *digital forensic* kepada audiens untuk memberitahukan kepada masyarakat bahwa *phishing* adalah penipuan yang dapat membobolkan data diri pribadi kita dan membuat masyarakat dapat kehilangan sejumlah uang dengan informasi pribadi yang didapatkan oleh pelaku.

#### 4. KESIMPULAN

Berdasarkan pembahasan terhadap rumusan masalah dan tujuan pada penelitian yang dibuat, maka ditarik kesimpulan sebagai berikut:

- 1) Berdasarkan hasil analisis *phishing* dari *email* menggunakan aplikasi linux dengan tools yang ada di dalam linux, dapat ditemukannya virus malware dengan menampakan bentuk *type*, *size file*, dan *subcategory* pada file *phishing* yang menunjukkan bahwa *subcategory* nya adalah *macro\_hunter* yang berarti file ini *malware* yang berbahaya.
- 2) Proses yang dilakukan menggunakan metode DFRWS memberikan tahapan-tahapan dapat mengumpulkan bukti digital yang relevan seperti URL *phishing*, alamat IP, dan informasi lain yang dapat membantu dalam investigasi kejahatan *cyber*.

#### UCAPAN TERIMA KASIH

Saya ucapkan terimakasih kepada yang terhormat bapak dan ibu dosen yang sudah banyak membantu saya dalam penyelesaian karya tulis ilmiah ini. Dan terimakasih kepada orang tua saya yang selalu support semua aktifitas perkuliahan saya hingga saya sampai kepada jenjang kelulusan yang di nanti-nanti.

## REFERENSI

- [1]. Vadila, N., & Pratama, A. R. I. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. *Automata*, 2(2)..
- [2]. Nofiyah, A., & Mushlihudin, M. (2020). *Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST)* (Doctoral dissertation, Universitas Ahmad Dahlan).
- [3]. Yudhana, A., Riadi, I., & Prasongko, R. Y. (2022). Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS). *Jurnal Informatika: Jurnal Pengembangan IT*, 7(1), 43-48.
- [4]. Suryana, A. L., El Akbar, R. R., & Widiyasono, N. (2016). Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS). *Jurnal Edukasi Dan Penelitian Informatika (JEPIN) Vol*, 2(2), 3-10.
- [5]. indah Fitria, E. (2023). Penerapan Digital Forensics Research Workshop Dalam Akuisisi Evidence Forensik Snack Video. *Jurnal Komputer Teknologi Informasi dan Sistem Informasi (JUKTISI)*, 2(2), 390-399.
- [6]. Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). Aspek yuridis kejahatan phishing dalam ketentuan hukum di Indonesia. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, 5(1).
- [7]. Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman cybercrime di indonesia: Sebuah tinjauan pustaka sistematis. *Jurnal Konstituen*, 5(1), 1-17.
- [8]. Rahmadian, F., Maksum, M., & Rambe, M. S. (2020). Perlindungan Nasabah Bank Terhadap Tindakan Phishing Studi Pada PT Bank Rakyat Indonesia (Persero) Tbk. *Journal Of Legal Research*, 2(2), 351-372.
- [9]. Anjheli, D. (2024). Privasi Digital dan Kejahatan Phishing di Indonesia: Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, 4(1), 165-189.
- [10]. Yustitiana, R. (2021). Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian dari Upaya Penegakan Hukum di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum. *Jurnal Hukum Visio Justisia*, 1(1), 98-126.
- [11]. Iskandar, O. (2024). Analisis Kejahatan Online Phishing Pada Masyarakat. *Leuser: Jurnal Hukum Nusantara*, 1(2), 32-36.
- [12]. Diniyah, K. J. (2022). Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Crime Phishing. *Dinamika*, 28(5), 3756-3775.
- [13]. Radiansyah, I., Rusdjan, C., & Priyadi, Y. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Journal of Innovation in Business and Economics*, 7(1), 1-14.
- [14]. Latifah, F. N., Mawardi, I., & Wardhana, B. (2022). Ancaman Pencurian Data (Phishing) Di Tengah Trend Pengguna Fintech Pada Pandemic Covid-19. *Islamic Banking and Finance Journal*, 6 (1), 73–85.
- [15]. Umar, R., Yudhana, A., & Fadillah, M. N. (2022). Analisis Forensik Aplikasi Dompok Digital Pada Smartphone Android Menggunakan Metode DFRWS. *KLIK-KUMPULAN JURNAL ILMU KOMPUTER*, 9(2), 265-278.