p-ISSN : 2406-7733
e-ISSN : 2597-9922

ANALISIS KEJAHATAN *PHISING* PADA SEKTOR *E-COMMERCE SHOPEE* MENGGUNAKAN METODE *NETWORK FORENSIC*

Nur Alya Gina[1], Sutarti[2]
Program Studi Sistem Komputer, Fakultas Teknologi Informasi, Universitas Serang Raya
Taman Drangong, Serang, Banten
Email: nuralyagina05@gmail.com[1], sutarti86@gmail.com[2]

Abstrak - Penggunaan *WhatsApp* sebagai *platform* media sosial populer telah membuat celah bagi pelaku kejahatan untuk melakukan aksinya seperti menyebarkan *phishing*. *Phishing* merupakan bentuk penipuan yang bertujuan untuk mendapatkan informasi sensitif seperti nama pengguna dan kata sandi. Dengan cara menyamar sebagai wujud nyata yang dapat dipercaya. Pelaku *phishing* melakukan aksinya dengan mengirimkan pesan *whatsapp* yang berupa pemberian koin *Shopee*, namun kenyataannya mengarahkan pengguna ke situs palsu yang dibuat oleh penipu. Penelitian ini bertujuan untuk melakukan investigasi dan analisis terhadap suatu kejahatan *phishing* dengan menggunakan metode *Network Forensic*. Adapun tahapan yang digunakan dalam penelitian ini yaitu proses akuisisi dan pengintaian, proses analisis, serta proses *recovery*. Penelitian dilakukan menggunakan *software wireshark* untuk mengambil data berupa file *capture* melalui jaringan *Wi-Fi* saat mengakses link *phishing* pemberian koin *shopee* kemudian *wireshark* menyaring data yang tertangkap seperti informasi singkat tentang paket, jumlah data yang didapat. Hasil dari penelitian ini, diperoleh informasi *fake domain* (*host phishing*) berupa DNS, *IP address*, *IP destination* serta TLSv1.2.

Kata Kunci: *Shopee, Network Forensic, Phishing, WhatsApp, Wireshark*

I. PENDAHULUAN

Di era ICT seperti sekarang, segala hal bisa dilakukan dengan mudah dan cepat. Hampir seluruh aspek kehidupan tidak terlepas dari teknologi informasi dan komunikasi. Hal ini dikarenakan teknologi internet memudahkan manusia dalam bertukar informasi secara cepat dan berkomunikasi dalam jarak jauh. Dengan memanfaatkan teknologi internet yang ada dapat memberikan kemudahan bagi pengguna dalam mengakses *website* atau aplikasi *web* bagi pengguna dalam melakukan aktivitas, salah satunya adalah melakukan transaksi jual beli online (*e-commerce*) (Andre, 2023).

Pada tahun 2023, jumlah pengguna *WhatsApp* mencapai 2,45 miliar orang di seluruh dunia. Hal ini mengukuhkan posisinya sebagai salah satu aplikasi pesan *instan* yang sangat diminati, termasuk di Indonesia. Namun, popularitas ini membuatnya menjadi sasaran empuk bagi pelaku penipuan online, terutama penipuan dengan metode *phishing* (eraspace.com, 2024).

Phishing adalah upaya untuk mendapatkan informasi sensitif. Dapatkan informasi pengguna melalui *email* atau situs *web* palsu. Dengan meniru tampilan *website* asli atau resmi. Penjahat menggunakan *email*, spanduk, atau *pop-up* untuk mengelabui pengguna agar mengarahkan mereka ke situs *web* palsu dan meminta mereka memberikan informasi sensitif seperti *username* dan *password*. Pada titik inilah penjahat memanfaatkan ketidaktahuan pengguna untuk mendapatkan informasi.

Penelitian ini dilakukan untuk menganalisis terkait kasus *phishing* yang ada pada *E-Commerce Shopee* berupa pesan *whatsapp* yang dibuat oleh pelaku dengan memberikan *link* yang berupa pemberian koin *shopee* yang mengarah ke situs *phishing*, Metode yang digunakan yaitu *Network Forensic* dikarenakan *phishing* biasanya melakukan serangan melalui komunikasi jaringan komputer. Sehingga dalam melakukan investigasi kasus *phishing*, jaringan komputer sangat diperlukan. Oleh karena itu, metode *Network Forensic* dapat digunakan untuk menginvestigasi serangan *phishing* dengan mengumpulkan dan menganalisis bukti digital yang terkait dengan komunikasi jaringan saat terjadi penyerangan.

Untuk melakukan analisis terhadap jaringan, diperlukannya *software Wireshark*. Dimana *Wireshark* merupakan aplikasi *open-source* yang digunakan sebagai analisis dalam pemecahan masalah lalu lintas jaringan. *Wireshark* dapat melakukan *capture* paket jaringan komputer dengan menghasilkan informasi data bukti kejahatan melalui analisis jaringan komputer (Agung Wijaya, 2023). Adapun jaringan yang digunakan pada penelitian ini yaitu dengan menggunakan jaringan *Wi-Fi*.

Penelitian ini bertujuan untuk melakukan investigasi dan analisis terhadap suatu kejahatan phishing yang telah terjadi dengan menggunakan metode *Network Forensic* dimana hasil yang didapat dari penelitian ini dapat mengungkap informasi *fake domain* (*host phishing*) berupa DNS, *IP address*, *IP destination* serta protokol TLSv1.2.

Dengan melakukan penelitian ini, dapat memberikan informasi untuk melakukan investigasi kasus *phishing* melalui jaringan dengan bantuan *software Wireshark*. Hasil investigasi yang telah dilakukan pada penelitian ini dapat memberikan

p-ISSN : 2406-7733
e-ISSN : 2597-9922

suatu bukti terkait aktifitas pencurian data melalui situs *phishing* sehingga dapat dilaporkan kepada pihak berwajib untuk menangani tindakan lebih lanjut.

II. TINJAUAN PUSTAKA

Penelitian mengenai kejahatan siber (cybercrime), khususnya serangan phishing, telah berkembang melalui berbagai pendekatan, seperti forensik digital, analisis lalu lintas jaringan, dan strategi pencegahan berbasis keamanan informasi. Dalam bidang forensik digital, Agil dan Mushlihudin (2020) menerapkan metode National Institute of Standards and Technology (NIST) untuk menginvestigasi pencurian data pribadi dan berhasil mengidentifikasi bukti digital berupa URL phishing, DNS, alamat IP, serta informasi yang berkaitan dengan penyerang. Pendekatan serupa dilakukan oleh Prasetyo et al. (2023) menggunakan metode National Institute of Justice (NIJ) untuk menganalisis serangan spear phishing melalui pemalsuan halaman Instagram dengan memanfaatkan penangkapan paket data jaringan. Sementara itu Prawira dan Samsudin (2022) menerapkan live forensics pada kasus email phishing dan menemukan bukti berupa informasi header email, alamat IP pengirim, serta malware Emotet. Ketiga penelitian tersebut menunjukkan bahwa pendekatan forensik digital dapat digunakan untuk mengumpulkan dan menganalisis bukti elektronik guna mengidentifikasi karakteristik serangan siber.

Selain investigasi forensik digital, analisis lalu lintas jaringan juga digunakan untuk mengidentifikasi aktivitas komunikasi dan potensi ancaman keamanan. Novita et al. (2021) memanfaatkan Wireshark untuk memantau penggunaan jaringan internet dalam lingkungan pembelajaran dan menunjukkan bahwa aplikasi tersebut mampu menyajikan informasi paket data secara terperinci. Rasyad et al. (2022) mengembangkan analisis serupa pada aplikasi Synology Chat dengan mengidentifikasi penggunaan protokol TLS 1.2 melalui port 443 serta perbedaan pola ukuran paket pada komunikasi personal chat, public group, dan private group. Hasil kedua penelitian tersebut memperlihatkan bahwa analisis paket jaringan dapat memberikan informasi mengenai karakteristik lalu lintas komunikasi, termasuk ketika isi pesan dilindungi oleh enkripsi.

Dalam aspek identifikasi ancaman dan pencegahan phishing, Ramadhan dan Nurnawati (2022) serta Puspitasari dan Sutabri (2023) menggunakan pendekatan literature review untuk mengkaji faktor penyebab serangan pada layanan e-commerce. Kedua penelitian tersebut mengidentifikasi rendahnya pengetahuan keamanan digital, faktor psikologis, penyalahgunaan informasi pribadi, dan penggunaan iming-iming hadiah sebagai faktor yang meningkatkan kerentanan pengguna. Sejalan dengan temuan tersebut, Kuswulandari et al. (2023) menggunakan pendekatan kualitatif untuk menganalisis risiko kejahatan siber pada pengguna WhatsApp, termasuk ancaman pencurian informasi pribadi, data perbankan, dan kode one-time password (OTP). Sementara itu, Nizar et al. (2023) menggunakan pendekatan Business Process Model and Notation (BPMN) untuk membahas mekanisme serangan phishing dan upaya perlindungan pengguna aplikasi dompet digital (e-wallet). Penelitian-penelitian tersebut menegaskan bahwa aspek perilaku pengguna, pemahaman terhadap mekanisme serangan, dan edukasi keamanan informasi memiliki peran penting dalam mengurangi risiko phishing.

Upaya penanganan ancaman phishing tidak hanya berfokus pada identifikasi serangan, tetapi juga mencakup tindakan mitigasi secara teknis. Sutarti et al. (2023) mengintegrasikan proses investigasi forensik digital melalui tahapan pengumpulan, pemeriksaan, analisis, dan pelaporan dengan penerapan router MikroTik untuk memblokir akses ke situs phishing. Penelitian tersebut berhasil mengidentifikasi informasi terkait pembuat situs berbahaya sekaligus melakukan pemblokiran sebagai langkah pencegahan pencurian data. Temuan ini menunjukkan bahwa hasil investigasi forensik dapat dimanfaatkan sebagai dasar penerapan mekanisme perlindungan jaringan.

Berdasarkan penelitian terdahulu, metode NIST, NIJ, dan live forensics berperan dalam pengumpulan serta pemeriksaan bukti digital, sedangkan analisis paket jaringan menggunakan Wireshark memberikan informasi mengenai karakteristik komunikasi dan aktivitas jaringan. Di sisi lain, pendekatan literature review, analisis risiko, dan pemodelan proses bisnis memberikan pemahaman mengenai faktor penyebab, mekanisme serangan, serta strategi pencegahan phishing. Dengan demikian, penelitian terdahulu menunjukkan bahwa investigasi forensik digital, analisis lalu lintas jaringan, dan mitigasi keamanan merupakan pendekatan yang saling melengkapi dalam menangani ancaman kejahatan siber.

Network Forensic

Forensik jaringan (*network forensic*) merupakan proses menangkap, mencatat dan menganalisis aktivitas jaringan guna menemukan bukti digital (*digital evidence*) dari suatu serangan atau kejahatan yang dilakukan terhadap, atau dijalankan menggunakan, jaringan komputer sehingga pelaku kejahatan dapat dituntut sesuai hukum yang berlaku. Forensik Digital dan Forensik Jaringan ini dapat digunakan untuk menemukan kejahatan di dunia maya seperti *cyber crime*. Karena meskipun kejahatan itu dilakukan secara digital tetap saja meninggalkan bukti atau "jejak".(Sutarti et al., 2023) Adapun Proses Forensik Jaringan dengan

p-ISSN : 2406-7733
e-ISSN : 2597-9922

menggunakan tiga tahapan (Ardiyasa et al., 2021) yaitu:

1. Akuisisi dan Pengintaian (*Reconnaissance*)
   Pada tahapan ini, aktifitas yang dilakukan yaitu pengumpulan informasi aktifitas *phishing* yang akan dianalisis. Dalam pengumpulan data, terdapat dua cara yaitu pengumpulan data dengan bekerja pada sistem online (data volatile) dan pengumpulan data dari disk yang terkait dengan aktifitas *phishing* secara *offline* dengan memanfaatkan berbagai *tools* (data *non- volatile*).
2. Analisis
   Pada tahapan ini, kegiatan yang dilakukan yaitu mengamati secara detail data yang diperoleh dari proses akuisisi, dengan cara menguraikan komponen-komponen pembentuknya atau penyusunnya untuk dikaji lebih lanjut. Analisis yang dilakukan meliputi: analisis aktifitas di jaringan komputer secara *online* maupun *offline*, analisis data rekaman jejak *phishing* (*volatile* atau *non-volatile*), analisis *log-file*, korelasi data dari berbagai perangkat pada jaringan yang dilalui serangan dan pembuatan *timeline* dari informasi yang diperoleh.
3. Recovery
   Pada tahap ini merupakan proses fase akhir yaitu penyajian informasi dari hasil investigasi yang telah dilakukan.

Teknik *Phising*

Penyerangan *phishing* yang dilakukan menggunakan beberapa teknik, diantaranya yaitu (exabytes.co.id, 2023):

a. Email *Phishing*: merupakan teknik yang dilakukan penyerang dengan mengirimkan *email* palsu yang meniru lembaga atau organisasi terpercaya.
b. *Spear Phishing*: Merupakan teknik serangan *phishing* yang ditargetkan secara khusus terhadap individu, organisasi, atau kelompok tertentu. Sebelum melakukan penyerangan, penyerang sudah terlebih dahulu melakukan riset yang mendalam tentang target mereka agar pesan yang mereka kirimkan dapat meyakinkan target.
c. *Whaling*: Tekniknya serupa dengan *spear phishing* namun pada *whaling* menargetkan individu yang lebih penting dalam suatu organisasi, seperti CEO atau CFO. Penyerang menggunakan informasi tentang target untuk membuat pesan yang lebih meyakinkan dan mengelabui target agar memberikan informasi sensitif.
d. SMS *Phishing* (*smishing*): Merupakan teknik dimana penyerang mengirimkan pesan teks (SMS) palsu yang berusaha untuk menipu penerima agar mengungkapkan informasi pribasi atau mengklik tautan berbahaya.
e. Voice *Phishing* (*vishing*): Merupakan teknik yang dilakukan oleh penyerang dengan menggunakan sambungan telepon untuk menipu targetnya.
f. *Pharming*: Merupakan teknik serangan dimana penyerang mencoba mengarahkan pengguna ke situs *web* palsu yang terlihat mirip dengan situs *web* yang sah.

Wireshark

Wireshark adalah perangkat lunak untuk menganalisis lalu lintas paket data yang dikirim melalui jaringan, dimana alat ini mampu menampilkan setiap paket dan detail isi paket. Administrator menggunakannya untuk menganalisis jaringan dan memecahkan masalah (Nur Saputro, 2024).

Fungsi Utama *Wireshark* yaitu merekam paket data dalam jaringan secara *real-time*. Selain itu, *wireshark* juga dapat menyimpan paket data kemudian menampilkan hasilnya melalui GUI yang sangat jelas. *Wireshark* juga digunakan sebagai alat untuk mendeteksi transfer berkas individu di dalam protokol tertentu. Adapun kegunaan *wireshark* yang lain yaitu dapat memisahkan dan melakukan pemecahan masalah jaringan serta sistem.

Protokol Jaringan

Protokol jaringan adalah aturan yang dibuat di dalam jaringan komputer yang harus dipenuhi oleh komputer pengirim dan juga komputer penerima agar proses komunikasi data dan pertukaran informasi bisa dilakukan meskipun keduanya memiliki sistem yang berbeda. Gampangnya, protokol jaringan adalah media yang menghubungkan antara satu komputer dengan komputer yang lain untuk saling berkomunikasi (domainesia.com, 2023).

Protokol jaringan yang biasa digunakan yaitu (Risyan, 2019):

a. *User* Datagram *Protocol* (UDP) merupakan protokol serupa dengan TCP namun UDP tidak membuat koneksi sebelum terjadinya transfer informasi. UDP digunakan untuk koneksi yang tidak terlalu kritis seperti transmisi audio/video (VoIP dan audio/video *streaming*).
b. *Transmission Control Protocol* (TCP) merupakan standar komunikasi yang dilakukan dengan membuat koneksi antara klien dengan server yang dituju dengan mengirimkan serta menerima informasi melalui jaringan. TCP bekerja dengan protokol internet untuk melakukan komunikasi. TCP cocok digunakan untuk koneksi yang membutuhkan keandalan tinggi seperti Telnet, HTTP, FTP, SSH.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

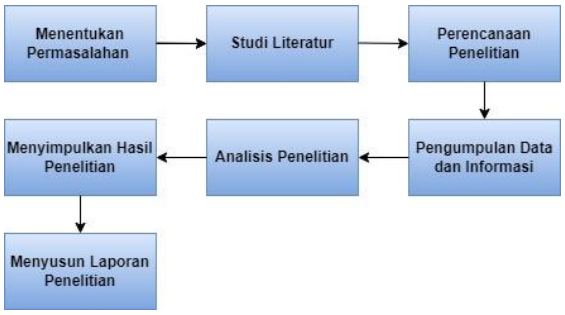
III METODOLOGI PENELITIAN

Tipe penelitian yang dilakukan menggunakan tipe penelitian terapan, dimana penelitian terapan bertujuan untuk melakukan pemecahan masalah sehingga hasil penelitian dapat dimanfaatkan untuk kepentingan manusia baik secara individu maupun kelompok.

Dalam kasus ini, penelitian dilakukan menggunakan teknik pengumpulan data melalui perekaman lalu lintas jaringan. Data yang diambil akan dianalisis menggunakan *software Wireshark* dengan melakukan *capture* paket data jaringan saat mengakses situs *phishing* untuk menemukan informasi dari penyerangan *phishing* berupa *fake domain* (*host phishing*) ditemukan berupa *IP address*, *IP destination*, dan protokol TLSv1.2.

Tahapan Penelitian

Untuk mendapatkan data yang akurat dan alur penelitian yang sesuai, maka perlu dibuat alur yang jelas untuk memperoleh data dan informasi yang lengkap untuk mendukung keabsahan materi dan pembahasan. Tahapan penelitian disajikan pada gambar 1.



Gambar 1. Diagram Alur Penelitian

1. Menentukan Permasalahan
   Tahapan awal yang dilakukan pada penelitian ini yaitu menentukan permasalahan yang akan dibahas yang bertujuan untuk mengidentifikasi permasalahan yang akan diteliti.
2. Studi Literatur
   Tahapan kedua yaitu melakukan studi literatur sesuai dengan topik yang diangkat. Kegiatan ini dilakukan untuk memperoleh informasi terkait penelitian yang akan dilakukan sehingga dapat memperkuat proses penelitian.
3. Perencanaan Penelitian
   Tahapan ketiga yaitu merencanakan proses-proses yang akan dilakukan dalam penelitian ini untuk memberikan hasil investigasi yang dilakukan. Perencanaan penelitian bertujuan agar pengujian ini dapat terlaksana secara sistematis.
4. Pengumpulan Data dan Informasi
   Tahapan keempat yaitu pengumpulan data dan informasi aktifitas *phishing* yang akan dilakukan dalam pengujian untuk melakukan investigasi penyerangan *phishing*.
5. Analisis Penelitian
   Tahapan kelima yaitu analisis penelitian dimana pada tahapan ini dilakukan analisis serangan *phishing* menggunakan metode *network forensic process* untuk menginvestigasi pelaku penyerangan *phishing*. Pada proses ini, penulis menggunakan *software Wireshark* untuk mengambil data berupa *file capture* melalui jaringan komputer yang sedang beroperasi kemudian menyaring data yang tertangkap.
6. Menyimpulkan Hasil Penelitian
   Tahapan keenam yaitu menyimpulkan hasil penelitian dimana ditampilkan hasil investigasi serangan *phishing* yang telah dianalisis kemudian dijelaskan hasil analisis yang berisi kesimpulan investigasi dari setiap *file capture*.
7. Menyusun Laporan Penelitian
   Tahap ini melakukan penyusunan laporan penelitian dengan menjelaskan secara terperinci tentang masalah yang diteliti, metode yang digunakan, hasil penelitian, dan penarikan kesimpulan.

Alat dan Bahan Penelitian

Dalam penelitian ini menggunakan beberapa alat dan bahan. Alat dan bahan yang dibutuhkan yaitu:

1. Kebutuhan *Hardware* / Perangkat Keras

Kebutuhan *Hardware* yang diperlukan pada penelitian ini yaitu menggunakan sebuah laptop dengan spesifikasi sesuai Tabel 1.

Tabel 1. Kebutuhan *Hardware* / Perangkat Keras

No	Item	Deskripsi
1	*Type*	Laptop
2	*Processor*	Intel Core i5 8Th Gen
3	*Memory* (RAM)	8.00GB
4	*Harddisk*	SSD 480GB & HDD 1TB

2. Kebutuhan *Software* / Perangkat Lunak

Kebutuhan *Software* yang diperlukan untuk penelitian ini antara lain:

1. *Wireshark* digunakan sebagai aplikasi untuk melakukan pengambilan data berupa *file capture* melalui jaringan komputer yang sedang beroperasi kemudian menyaring data yang tertangkap. Menggunakan *Wireshark* versi V.4.2.5
2. *Whatsapp* digunakan sebagai media untuk pengambilan data berupa pesan terkait kasus phishing. Menggunakan *Whatsapp* versi 24.15.1

p-ISSN : 2406-7733
e-ISSN : 2597-9922

3. Google Chrome digunakan untuk membuka link *phishing* dan melakukan pemeriksaan terhadap *domain*. Menggunakan *Google Chrome* versi 64-bit
4. *Windows* digunakan sebagai sistem operasi yang digunakan pada laptop dengan jenis *Windows*10 versi 21H2 – 64 bit.

Tabel 2. Kebutuhan *Software* / Perangkat Lunak

No	Nama Aplikasi	Versi	Deskripsi
1.	Wireshark	V.4.2.5	Aplikasi yang digunakan untuk melakukan analisis terhadap jaringan yang sedang beroperasi.
2.	Whatsapp	24.15.1	Aplikasi yang digunakan sebagai media dalam mengambil data.
3.	Google Chrome	64-bit	Digunakan untuk membuka dan pemeriksaan situs phishing.
4.	Windows OS	Windows10 versi 21H2	Sistem operasi yang digunakan oleh laptop.

Data Penelitian

Penelitian ini menggunakan data primer, yaitu data yang didapatkan peneliti melalui sebuah pesan *whatsapp* berupa link *phising*, data tersebut yang akan dianalisis dalam penelitian ini.

Adapun data sekunder yang digunakan yaitu melalui pesan pada akun *whatsapp* korban kejahatan *phishing* yang menjadi data tambahan bahwa serangan *phishing* benar adanya dan kejahatan ini sangat merugikan.

Deskripsi Usulan Penelitian

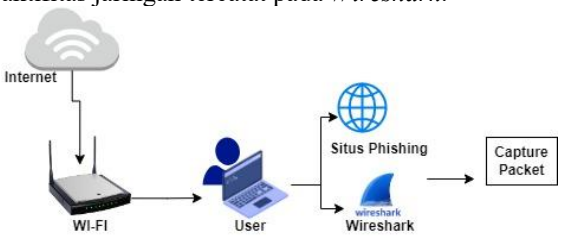
Berdasarkan pesan yang di terima pada aplikasi *whatsapp* berupa pemberian koin *shopee* Terdapat sebuah link untuk mengklaim koin tersebut Namun saat mengakses link tersebut terdapan perintah *login* akun *shopee*. Pasalnya, pada link berbagi koin *shopee* resmi, jika mengakses link tersebut namun belum memiliki aplikasi *shopee*, akan diarahkan menuju situs *shopee* resmi yang menyediakan untuk menginstal aplikasi tersebut, adapun jika aplikasi *shopee* sudah terinstal, saat membuka link akan diarahkan langsung menuju aplikasinya tanpa mengharuskan *login* akun. Sedangkan pada pesan *whatsapp* yang membagikan koin *shopee* tersebut merupakan link palsu atau lebih sering dikenal dengan sebutan *phishing*.

Penelitian ini bertujuan untuk melakukan investigasi dan analisis kasus *phishing* yang dikirimkan melalui pesan *whatsapp* tersebut. Dalam penelitian ini menggunakan metode *network forensic* dengan *software Wireshark* yang akan melakukan *capture* paket data jaringan komputer untuk menemukan informasi *fake domain* (*host phishing*) serta protokol TLSv1.2

Perancangan Usulan Penelitian

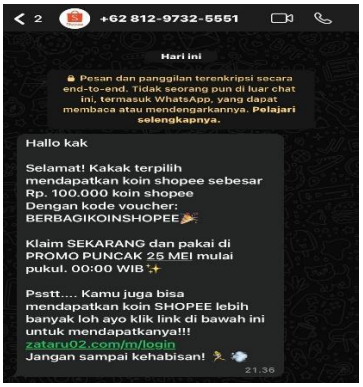
Perancangan arsitektur jaringan yang akan digunakan dalam penelitian ini membutuhkan internet sebagai konektivitas PC *user* agar *user* dapat mengakses situs yang akan dituju. Adapun *software Wireshark* yang digunakan untuk melalukan *capture* paket jaringan komputer saat user megakses situs *Phishing*.

Rangkaian yang dilakukan yaitu ketika pc *user* telah terhubung internet melalui jaringan *Wi-Fi*, user mengaktifkan *capture* paket pada *Wireshark* kemudian mengakses tautan link yang tercantum pada pesan *whatsapp* yang mengarah ke situs *phishing*, setelah itu informasi yang didapatkan pada aktifitas jaringan tercatat pada *Wireshark*.



Gambar 2. Rangkaian Alur Analisis

Adapun kasus *phishing* yang akan dianalisis merupakan pesan yang didapatkan pada apikasi *whatsapp* dari nomor +6281297325551 yang menyebarkan *phishing* dengan motif pemberian koin *shopee* terdapat kutipan link. Pesan ditunjukan dengan gambar 3.



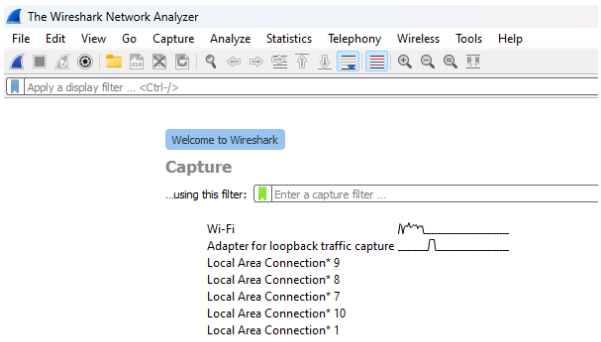
Gambar 3. Kasus *Phishing*

Rancangan Pengujian

Pengujian dimulai dengan melakukan *capture* paket jaringan komputer dengan menggunakan *Wireshark*, tahapan yang akan dilakukan yaitu:

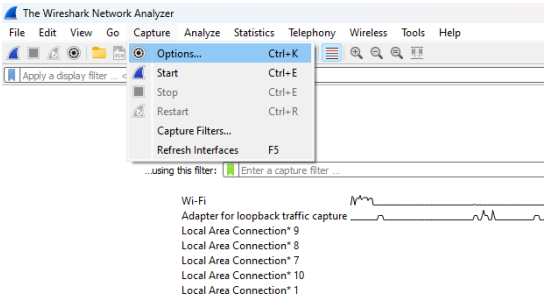
1. Menjalankan aplikasi *Wireshark* untuk melakukan *capture* paket.

p-ISSN : 2406-7733
e-ISSN : 2597-9922



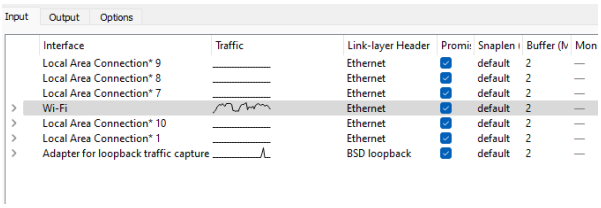
Gambar 4. Tampilan *Interface Wireshark*

2. Pilih kolom *Capture* dan klik pilihan *Options* untuk memilih *interface* yang akan dilakukan pengcapturan. Alternatifnya klik dua kali pada pilihan *interface*. Sebelumnya koneksikan laptop dengan jaringan internet terlebih dahulu.



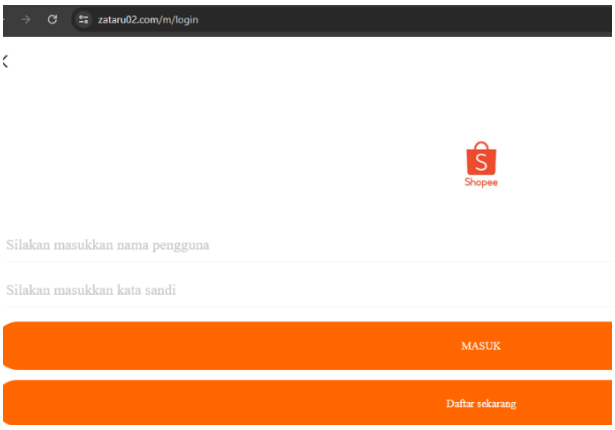
Gambar 5. Pemilihan *Interface*

3. Pilih *interface* yang akan di *capture*. Pada penelitian ini *interface* yang akan dimonitoring yaitu melalui *Wi-Fi*, maka klik bagian *Wi-Fi*. Selanjutnya klik *Start* untuk memulai.



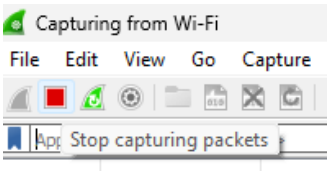
Gambar 6. Pemilihan *Interface Wi-Fi*

4. Disela *Wireshark* berjalan, akses link *phishing* yang terdapat pada pesan *whatsapp* pemberian koin oleh nomor +6281297325551. Tampilan awal saat akses situsnya terdapat perintah untuk *login* akun *shopee* yaitu memasukkan nama pengguna dan kata sandi yang tertaut dengan akun *shopee*.



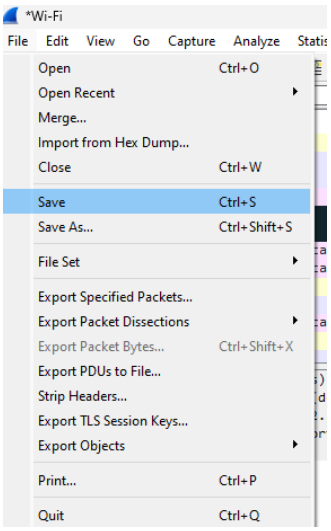
Gambar 7. Tampilan Awal Perintah *Login*

5. Kembali ke program *Wireshark* yang telah dijalankan dengan *interface Wi-Fi*, setelah *Wireshark* melakukan pengcapturan. Kemudian klik tanda yang berwarna merah untuk menyelesaikan *capture* paketnya.



Gambar 8. Stop *Capture*

6. Selanjutnya simpan hasil *capture* dengan mengklik pilihan file, dan *Save* atau *Save As*. File yang telah tersimpan pada perangkat komputer berbentuk file *pcapng.



Gambar 9. Penyimpanan Hasil *Capture*

p-ISSN : 2406-7733
e-ISSN : 2597-9922

IV HASIL DAN PEMBAHASAN

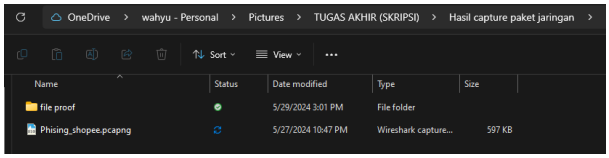
Hasil dari penelitian ini yaitu hasil pengujian melalui tahap proses akuisisi dan pengintaian, serta analisis dan *recovery*.

Hasil Pengujian

Pada pengujian awal dilakukan dengan mengcapture paket data jaringan *Wi-Fi* pada *Wireshark*. Pengujian ini merupakan tahapan dari metode *Network Forensic* yaitu proses Akuisisi dan pengintaian untuk mengumpulkan data terkait kasus *phising*, kemudian proses Analisis untuk mengamati data hasil *capture*.

A. Akuisisi dan Pengintaian (*reconnaissance*)

Hasil dari proses akuisisi dan pengintaian didapatkan data non-*volatile* dengan nama file (Phising_shopee.pcpapng) yang berisi informasi *capture* paket data jaringan *Wi-Fi* saat akses situs *phising* yang dilakukan pada tanggal 27 Mei 2024 dengan file *type* berbentuk *Wireshark capture* file, adapun berkas file *proof* merupakan file bukti yang berisi *screenshoot* pada aplikasi *whatsApp* korban, layar hasil pencarian *domain* pada centralops.net, serta tangkapan layar hasil saat melakukan ping pada *domain* dengan cmd.



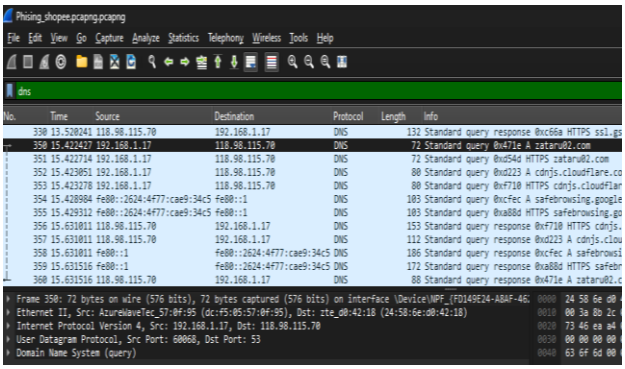
Gambar 10. Akuisisi Data

B. Analisis

Setelah data penelitian terkumpul melalui proses akuisisi dengan hasil *capture* paket jaringan komputer pada *Wireshark*. Selanjutnya proses investigasi yang akan dilakukan yaitu menganalisis mengenai informasi yang telah ditemukan melalui hasil *capture* paket tersebut. Adapun informasi yang ditemukan yaitu:

1. Protokol DNS (*Domain* Name System)

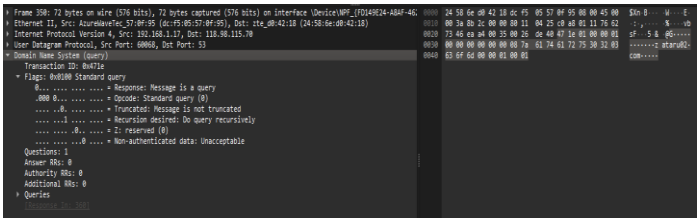
Pada file Phising_shopee.pcapng, informasi yang tercatat melalui protokol DNS sebanyak 54 Paket data. Untuk lebih mudah dalam melakukan analisis, digunakan *filterisasi* dengan mencantumkan 'dns' untuk mencari informasi terkait aktifitas serangan atas mengakses ke situs *phising shopee* terdapat paket nomor 350 dengan protokol DNS yang melakukan *query request* kepada zataru02.com/m/login.



Gambar 11. Hasil *Request Protocol* DNS

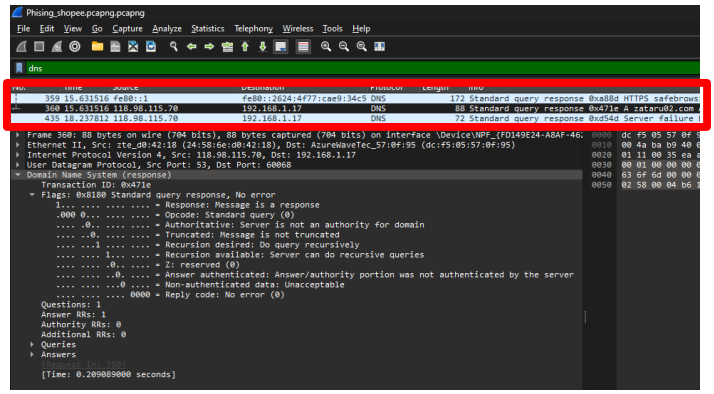
Informasi yang tercatat pada panel detail paket yaitu:

a) *Frame* 350: 72 *bytes* menunjukkan pada paket data nomor 25 dengan panjang paket 72 *bytes*.
b) *Ethernet* II, src Azurewav_57:0f:95 (dc:f5:05:57:0f:95), dst: zte_d0:42:18 (24:58:6e:d0:42:18). Menunjukkan mac dari *source* yaitu dc:f5:05:57:0f:95 dan mac dari mac *destination* 24:58:6e:d0:42:18.
c) *Internet Protocol Version* 4, src: 192.168.1.17, Dst: 118.98.115.70. Menunjukkan Versi 4 dengan IP *source* 192.168.1.17 dan IP *Destination* 118.98.115.70.
d) *User Datagram Protocol* dengan *source port* 60068 dan *destination port* 53.
e) *Domain Name System.*



Gambar 12. Detail *Query* DNS

Selanjutnya paket data nomor 360 merupakan *respon* dari paket data nomor 350 dimana hasilnya menunjukan bahwa *respon* DNS *query* zataru02.com/m/login dengan *IP address source* 118.98.115.70 dan *IP destination* 192.168.1.17.



Gambar 13. Hasil Respon DNS *Server*

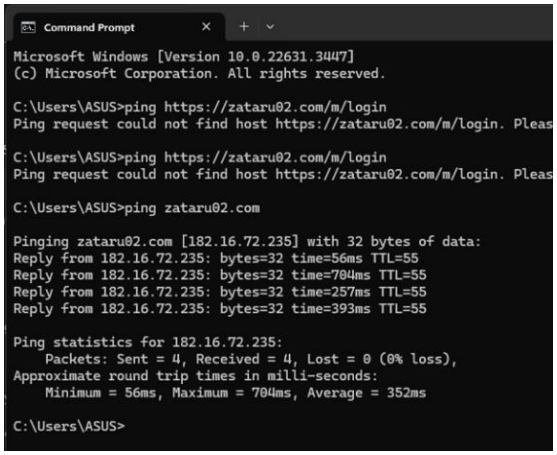
p-ISSN : 2406-7733
e-ISSN : 2597-9922

Setelah menganalisis protokol DNS ditemukan *IP source* 192.168.1.17 yang merupakan *IP address* dari jaringan *wifi* yang digunakan peneliti dan *IP destination* yang tercatat bukan *IP address* dari *domain* yang dituju melainkan *IP server* DNS publik yang dimiliki oleh PT. Telkom Indonesia yaitu 118.98.115.70, hal ini karena perangkat yang digunakan telah dikonfigurasi secara otomatis menggunakan *server* DNS tersebut.
Selanjutnya dilakukan pencarian informasi lebih lanjut terkait *Domain* tersebut menggunakan *dnslookup* yang tersedia pada *website* https://centralops.net. Dengan melakukan pencarian menggunakan *domain* zataru02.com/m/login, menghasilkan informasi yang didapatkan yaitu satu *IP address* server 182.16.72.235 yang merupakan *IP address* dari *domain* zataru02.com/m/login



Gambar 14. Hasil IP address domain

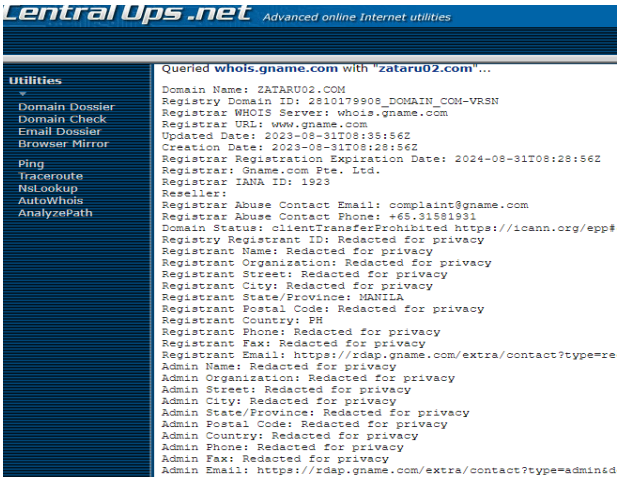
Melalui pengecekan ping pada cmd kepada situs zataru02.com/m/login hasil *IP* yang muncul sesuai dengan hasil *IP dnslookup* pada centralops.net yaitu 1182.16.72.235.



Gambar 15. Ping CMD

Adapun informasi *Domain Whois Record* yang berhubungan dengan *domain* zataru02.com diperoleh hasil:

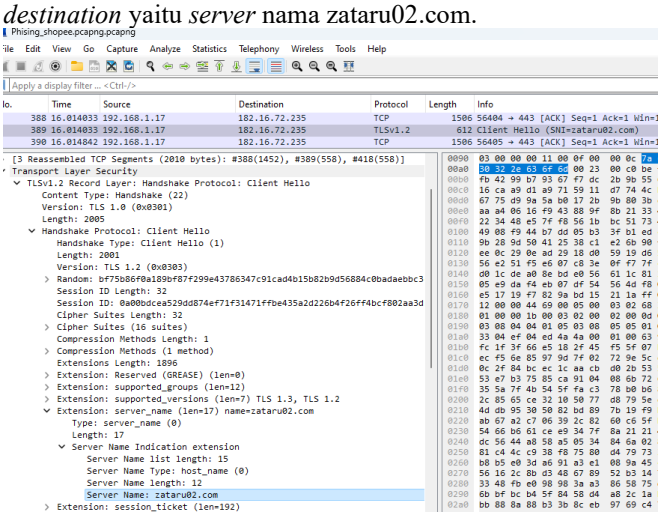
a. Nama domain: zataru02.com
b. Pebuatan *domain*: 31 Agustus 2023
c. Provinsi pendaftar: Manila
d. Negara pendaftar: Filipina (PH)



Gambar 16. Hasil Domain Whois Record

2. *Client Hello*

Selanjutnya pada file Phising_shopee.pcapng menyimpan informasi paket data berupa protokol TLSv 1.2 seperti yang tercatat pada paket data nomor 389 dengan protokol TLSv 1.2 sebagai *record layer handshare protocol "Client Hello"* dimana protokol ini merupakan komunikasi *client* ke *server* awal. Komunikasi ini dikirim oleh *client* dengan *IP address* 192.168.1.17 kepada *server* dengan *IP* 182.16.72.235 untuk memulai sesi dengan *server*. Pengiriman komunikasi dari *IP address* 192.168.1.17 dengan mengirimkan permintaan *cipher suites* sebanyak 16 *suites*. Dari ke-16 *suites* yang dikirimkan, hanya satu *suites* yang disetujui, untuk mengamankan komunikasi menggunakan protokol TLSv 1.2. *Server* yang disetujui oleh *IP destination* yaitu *server* nama zataru02.com.



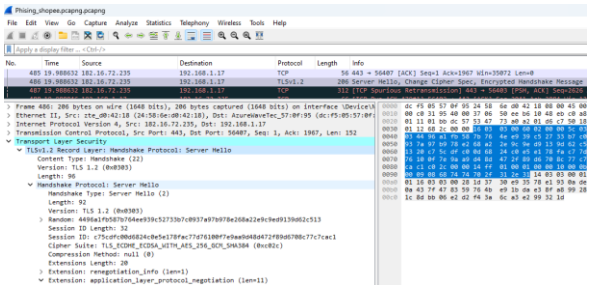
Gambar 7. Hasil Protokol TLSv 1.2 "Client Hello"

3. *Server Hello*

Masih dengan protokol TLSv 1.2, informasi yang didapat setelah *client* mengirim permintaan kepada *server* yaitu *record layer protokol "Server Hello"* menggunakan protokol TLSv 1.2 dalam menyetujui permintaan komunikasi dari *client* dengan *IP* 192.168.1.17 pada paket data nomor 486 kepada *server IP* 182.16.72.235. Hasil persetujuan

p-ISSN : 2406-7733
e-ISSN : 2597-9922

komunikasi menggunakan *suites* TLS_ESDHE_ECDSA_WITH_AES_256_GCM_SHA384 yang bernilai (0x02c).



Gambar 18. Hasil Protokol TLSv1.2 "Server Hello"

C. Recovery

Proses akhir yang dilakukan adalah pemulihan (*Recovery*) dengan menyampaikan informasi dari hasil investigasi dan analisis file Phising_shopee.pcapng. Hasil analisis menunjukkan bahwa protokol jaringan terlibat saat mengakses link phising *Shopee*, yang disajikan dalam tabel 3.

Tabel 3. Laporan Hasil Investigasi dan Analisis

Paket Data	Hasil
Paket Data Nomor 350 dan 360	• Protokol DNS (*Domain Name System*) • *Host phishing*: zataru02.com/m/login • *IP address source*: 192.168.1.17 • *IP address destination*: 118.98.115.70 • *IP address host Phishing*: 182.16.72.235 • Nama *domain*: zataru02.com • Pembuatan *domain*: 31 Agustus 2023 • Provinsi pendaftar: Manila • Negara pendaftar: Filipina (PH)
Paket Data Nomor 389	• Protokol TLSv1.2 • *Handshake* protokol: *Client Hello* • Nama *Request server*: zataru02.com • *IP address source*: 192.168.1.17 *request to IP address destination*: 182.16.72.235 • *Send request chipper suites*: 16 *suites*
Paket Data Nomor 486	• Protokol TLSv1.2 • *Handshake* protokol: *Server Hello* • Nama *Respon server*: zataru02.com • *IP address source*: 182.16.72.235 *respon to IP address destination*: 192.168.1.17 • Cipher suites terpilih: TLS_ESDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0x02c)

Pembahasan Penelitian

Dalam penelitian ini, proses investigasi dan analisis difokuskan pada serangan *phishing* yang dikirim melalui pesan *WhatsApp* dengan nomor +6281297325551. Pelaku mengirimkan pesan pembagian koin *shopee* dengan tautan zataru02.com/m/login, yang merupakan situs *Shopee* palsu yang dirancang oleh pelaku. Karena penelitian yang dilakukan menginvestigasi *phising* melalui jaringan, metode *Network Forensic* digunakan dalam penelitian ini. Adapun jaringan yang digunakan dalam penelitian ini yaitu *WI-FI*.

Pengujian ini menghasilkan data non-*volatile* dari proses akuisisi dan pengintaian yang menggunakan *Wireshark* untuk mengambil hasil *capture* paket jaringan komputer. File yang disimpan dengan nama file Phising_shopee.pcapng berisi informasi *capture* paket data jaringan komputer saat mengakses situs *phishing* pada tanggal 27 Mei 2024, dan juga memiliki file *proof* sebagai bukti tambahan untuk melakukan investigasi kasus *Phishing*.

Adapun protokol-protokol yang diamati yaitu protokol DNS yang dihasilkan saat pertama kali mengakses link yang dikirimkan melalui pesan *whatsapp* oleh +6281297325551 dimana protokol ini menampilkan *query request* yang dikirimkan oleh IP 192.168.1.17 (*IP address* peneliti) serta respon yang dikirimkan oleh server DNS. Protokol selanjutnya yang didapatkan yaitu TLSv1.2 dimana penyerangan *phishing* yang dilakukan menggunakan protokol TLS untuk menjadikan situsnya terpercaya.

Selain menganalisis hasil capture pada *Wireshark*, penelitian ini juga mencari dan melakukan ping ke *domain* yang digunakan pelaku melalui centralops.net. Hasil yang diperoleh berupa informasi alamat *IP server* dari *domain* tersebut. Sedangkan untuk centralops.net, kami menemukan hasil *whois record* untuk nama *domain* tersebut. Informasi yang diperoleh adalah bahwa nama *domain* tersebut dibuat pada tanggal 31 Agustus 2023 yang berlokasi di provinsi Manila, Philifina.

Setelah melakukan investigasi serta analisis terkait kejahatan *phishing* koin *shopee* yang dilakukan pada *Wireshark* untuk meng*capture* paket data jaringan komputer dengan pemanfaatan jaringan *Wi-Fi* telah memberikan informasi bahwa pelaku menyerang target untuk mengirimkan informasi akun *Shopee* target melalui *link* yang dikirimkan pada pesan *whatsapp* dengan nomor +6281297325551. Dengan menggunakan *domain* zataru02/m/login dimana pada domain tersebut, *IP* yang digunakan yaitu 182.16.72.235. Terdapat protokol TLS dimana pelaku menggunakan TLS untuk mengamankan situsnya.

Kelebihan menggunakan *Wireshark* untuk melakukan analisis serangan *phishing Shopee* adalah bahwa itu dapat menganalisis paket data melalui jaringan saat mengakses link *phishing* dilakukan secara *real-time* dan memberikan informasi detail. Meskipun demikian, karena *software* ini berbasis *open-source*, saat mengambil paket, *Wireshark* hanya dapat menganalisis aktifitas jaringan *Wi-Fi* yang dilakukan oleh perangkat yang menjalankan *Wireshark* saja walaupun perangkat lain terhubung dengan jaringan yang sama.

p-ISSN : 2406-7733
e-ISSN : 2597-9922

Analisis terhadap serangan *phishing* yang dikirimkan melalui pesan pada aplikasi *whatsapp* telah berhasil menemukan informasi fake *domain* (*host phishing*) seperti DNS beserta *IP* yang digunakan oleh *domain* tersebut, adapun protokol TLSv1.2 yang digunakan pelaku untuk mengamankan situs *phishing*nya. pada saat peneliti mencari protokol HTTP pada *software wireshark* tidak ditemukan protokol HTTP sehingga penelitian ini belum dapat menemukan informasi personal pelaku.

V PENUTUP

Kesimpulan

Berdasarkan penelitian yang telah dilakukan, hasilnya adalah:

1. Dengan menggunakan *Wireshark*, penelitian ini dapat menyelidiki serangan *phishing* melalui pemantauan jaringan saat mengakses situsnya. *Wireshark* merekam paket data pada jaringan *Wi-Fi* untuk mengumpulkan informasi tentang aktivitas penyerangan *phishing*.
2. Penerapan metode *Network Forensic* dalam penelitian ini berhasil menemukan informasi dari penyerangan *phishing* koin *shopee* berupa *fake domain* (*host phishing*) yaitu zataru02.com.m/login. dengan *IP address* 182.16.72.235. Selain itu tercatat bahwa pelaku menggunakan protokol TLSv1.2 untuk mengamankan situsnya agar informasi yang dikirimkan tidak dapat dilihat oleh pihak yang tidak berwenang.

Saran

Berdasarkan hasil kesimpulan yang telah diperoleh, terdapat saran yang dapat dilakukan untuk penelitian selanjutnya. Adapun saran yang diberikan yaitu :

1. Karena hanya *Wireshark* yang digunakan dalam penelitian ini, sehingga hanya dapat menganalisis aktifitas jaringan *WI-FI* yang beroperasi melalui device.
2. Perlu dilakukan penelusuran atau pencarian informasi lebih *detail* Ketika diperoleh suatu informasi *fake domain*.

DAFTAR PUSTAKA

Agil, N., & Mushlihudin. (2020). Analisis Forensik pada Web Phisihing Menggunakan Metode National Institute Of Standards And Technology (NIST). *Jurnal Sarjana Teknik Informatika*, *8, No.2*(2336–5197), 11–23.

Agung Wijaya. (2023, July). *Apa itu Phishing?* Dianisa.Com. https://dianisa.com/pengertian-phishing/

Andre, D. (2023, April). *Perkembangan Teknologi Informasi : Dampaknya Sampai Saat Ini*. Toffeedev.Com.

Ardiyasa, W., Luh, N., Suwirmayanti, G. P., Teknologi, I., Bisnis, D., & Bali, S. (2021). *Analisa Serangan Remote Exploit pada Jaringan Komputer dengan menggunakan Metode Network Forensic*.

domainesia.com. (2023). *Kupas Tuntas Protokol Jaringan dari Pengertian Hingga Jenisnya!*

Dwi Prasetyo, A., Bayu Seta, H., Wayan Widi, I. P., Ilmu Komputer, F., Pembangunan Nasional Veteran Jakarta, U., Fatmawati No, J. R., Labu, P., & Selatan, J. (2023). Analisis Digital Forensik Spear Phishing Menggunakan Metode National Institute of Justice (Studi Kasus: Instagram Verified Account). *Jurnal Informatik Edisi Ke-19*.

eraspace.com. (2024). *Penipuan di Whatsapp dengan Modus Phishing yang Semakin Marak*. Eraspace.Com. https://eraspace.com/artikel/post/penipuan-di-whatsapp-dengan-modus-phishing-yang-semakin-marak

exabytes.co.id. (2023). *Teknik Phishing Paling Umum*.

Faradilla A. (2023, February 22). *Apa Itu IP Address? Pengertian, Jenis, dan Fungsinya*. Https://Www.Hostinger.Co.Id/Tutorial/Apa-Itu-Ip-Address#IPv4. https://www.hostinger.co.id/tutorial/apa-itu-ip-address#IPv4

Ginee.com. (2021, October). *Sejarah Shopee di Indonesia: Marketplace Sukses di Tanah Air*. https://ginee.com/id/insights/sejarah-shopee-indonesia/

Kuswulandari, R., Wirid, A., Jowanka, I., Nabila, T., Riyanto, P., & Listiani, T. (2023). *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Aplikasi Whatsapp*.

Kuswulandari, R., Wirid, A., Nabila, T., & Listiani, T. (2023). *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Aplikasi Whatsapp*.

M Falah. (2018). *Apa Itu WhatsApp dan Kelebihanya*.

Mamad, J. (2024). *Tutorial Lengkap: Cara Menggunakan Wireshark Terbaru*. Www.Centerklik.Com.

Nizar, M., Zahra, A. N., Darmawan, M. Z., Abdillah, R., & Anaking, P. (2023). Analisis Modus Penipuan Digital Teknik Phising melalui Aplikasi WhatsApp Menggunakan Metode BPMN (Studi Kasus Pada Peretasan E-Wallet). *Seminar Nasional Sistem Informasi*.

Nur Saputro. (2024). *Kenali Pengertian Wireshark Beserta Fungsi dan Cara kerjanya, Lengkap!*

Paul Gillin. (n.d.). *Sejarah phishing*. Retrieved December 2, 2023, from

p-ISSN : 2406-7733
e-ISSN : 2597-9922

https://www.verizon.com/business/resources/articles/s/the-history-of-phishing/

Prawira, Y., & Samsudin. (2022). Live Forensics Analysis Of Malware Identified Email Crimes To Increase Evidence Of Cyber Crime. *Jurnal Teknologi Informasi Dan Komunikasi*, *13*. https://doi.org/10.31849/digitalzone.v13i2.11570

Puspitasari, D., & Sutabri, T. (2023). Analisis kejahatan phising pada sektor e-commerce di marketplace shopee. *Jurnal Digital Teknologi Informasi*, *6*(2). https://doi.org/10.32502/digital.v6i2.5653

Ramadhan, I. H., & Nurnawati, E. K. (2022). Analisis Ancaman Phishing Dalam Layanan E-Commerce. *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST)*. https://doi.org/10.34151/prosidingsnast.v8i1

Rasyad, G. Y., Hariyadi, D., & Febrianto, T. (2022). *Analisis Lalu Lintas Jaringan Terenkripsi Dari Secure Instant Messaging Application: Studi Kasus Pada Aplikasi Pesan Instan Synology Chat* (Vol. 5, Issue 2).

Redaksi OCBC NISP. (2023). *Apa itu Phising? Pengertian, Jenis, dan Cara Menghindarinya*.

Risyan, R. (2019, September). *Pengertian, Fungsi, Dan Jenis-Jenis Protokol Jaringan*.Www.Monitorteknologi.Com. https://www.monitorteknologi.com/protokol-jaringan/

Sutarti, Siswanto, & Bachtiar, A. (2023). Analisis Web Phishing Menggunakan Metode Network Forensic Dan Block Access Situs Dengan Router Mikrotik. *Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST) 2022*.

Tri Novita, R., Gunawan, I., Marleni, I., Gregarius Grasia, O., & Nanda Valentika abcde Teknik Elektro Sekolah Tinggi Teknologi Ronggolawe Cepu Penulis Korenspondensi, M. (2021). Analisis Keamanan Wifi Menggunakan Wireshark. In *Jurnal Elektro Smart)* (Vol. 1, Issue 1). https://www.researchgate.net/publication/316464159_Analisis_Keama