JTINFO

JURNAL TEKNIK INFORMATIKA, Vol.3 No.1 Febuari 2024
E-ISSN**:** 2528-2247

ANALISIS *WEB PHISHING* MENGGUNAKAN METODE OSCAR FORENSIC (STUDI KASUS : FOLLOWER INSTAGRAM GRATIS)

PHISHING WEB ANALYSIS USING THE OSCAR FORENSIC METHOD (CASE STUDY: FREE INSTAGRAM FOLLOWERS)

Dika Agustian Akbar[1*], Muhammad Rahdian Ega Kurnia[2], R.M. Genggam Satoe Bintang[3], Rahmat Purwoko[4]

[1,2,3,4]Politeknik Siber dan Sandi Negara
Email : [1*]dkgusti4k@gmail.com, [2]muhammad.rahdian@student.poltekssn.ac.id,
[3]rm.genggam@student.poltekssn.ac.id, [4]rahmat.purwoko@poltekssn.ac.id

Abstrak

Media sosial telah menjadi alat utama untuk interaksi antar pengguna dan penyebaran informasi. Dampaknya mencakup persaingan untuk mendapatkan perhatian di platform seperti Instagram, yang mengakibatkan masalah seperti penipuan akun, pencurian data pribadi, dan perdagangan akun hasil retas. Salah satu jenis kejahatan yang umum terjadi adalah spear phishing, di mana penjahat menciptakan halaman palsu yang menyerupai platform asli untuk menipu pengguna. Digital forensik menjadi kunci dalam menemukan bukti digital terkait kejahatan ini. Penelitian ini fokus pada analisis digital forensik terkait tindak spear phishing dengan menggunakan metode OSCAR, yang mencakup tahapan *Obtain information, Strategize, Collect evidence, Analyze, dan Report*. Hasil penelitian mengidentifikasi laman phishing dengan domain pelaku phishing. Metode OSCAR memberikan panduan sistematis untuk menyelidiki dan melaporkan tindakan kejahatan phishing ini dengan menggunakan pendekatan forensik yang efektif.

Kata Kunci: Instagram, Phishing, Metode OSCAR

Abstract

Social media has become a major tool for interaction between users and dissemination of information. The impact includes competition for attention on platforms like Instagram, resulting in problems such as account fraud, theft of personal data, and trading in hacked accounts. One common type of crime is spear phishing, where criminals create fake pages that resemble genuine platforms to deceive users. Digital forensics is the key to finding digital evidence related to this crime. This research focuses on digital forensic analysis related to spear phishing using the OSCAR method, which includes the Obtain information, Strategize, Collect Evidence, Analyze, and Report stages. The research results identified phishing pages with the domain of the phisher. The OSCAR method provides a systematic guide to investigating and reporting these phishing crimes using an effective forensic approach.

Keywords: *Instagram, Phishing, OSCAR Method*

1. PENDAHULUAN

Memasuki zaman yang semakin modern, kini mengacu pada dunia digital, begitu pula Ilmu Pengetahuan dan Teknologi. Dampaknya terasa signifikan dalam berbagai aspek kehidupan, terutama dalam berbagai media yang ada seperti media sosial. Tercatat 167 juta orang Indonesia pada Januari 2023 telah aktif menggunakan media sosial (Widi, 2023). Fenomena ini menjadikan orang Indonesia berlomba-lomba dalam menambah *follower* gratis (Rizka, 2023). Berbagai cara dilakukan seperti melakukan pembelian *follower*, meminta teman untuk memfollow, dan bahkan melakukan pencarian terhadap situs *follower* Instagram gratis.

Fenomena penambahan *follower,* membuat suatu kerentanan baru bagi

pengguna karena pengguna mungkin cenderung kurang waspada terhadap akun yang baru diikuti, terutama jika pertambahan tersebut terjadi secara drastis dalam waktu singkat. Serangan *phishing* melalui penambahan follower dapat dilakukan dengan memberikan iming-iming terhadap *follower* dengan waktu yang singkat. Kerentanan pengguna ini dimanfaatkan oleh penjahat cyber untuk melakukan penetrasi terhadap perangkat pengguna yang telah mengakses tautan tersebut.

Pengguna seringkali tidak menyadari bahwa peningkatan jumlah follower yang signifikan dapat mengekspos mereka pada risiko serangan *phishing* yang lebih tinggi, karena upaya ini seringkali terjadi di latar belakang tanpa pemberitahuan yang jelas. Para penyerang dapat menggunakan situs web gratis untuk mengejar penambahan follower secara massal dengan menawarkan layanan tersebut tanpa biaya, sehingga menarik perhatian pengguna yang mungkin mencari cara cepat untuk meningkatkan popularitas akun mereka.

Berkaitan dengan *follower* Instagram, penelitian sebelumnya telah menggali informasi *forensic social media* yang menjelaskan terkait dengan serangan DDoS yang dilakukan dari luar sistem terhadap Facebook, Myspace, Twitter, LinkedIn, dll (Shaw et al., 2016). Penelitian lainnya oleh Humaira A. dkk. dilakukan beberapa studi literatur dalam berbagai forensik jaringan terhadap social network seperti social media (Arshad et al., 2020). Sementara itu, penelitian oleh Heather J. dkk. menunjukkan terkait beberapa peristiwa phishing yang terjadi pada media sosial sebagai akibat kebiasaan online, pemrosesan informasi, demografi (Parker & Flowerday, 2020). Sejalan dengan konteks penelitian ini, peneliti melakukan forensic jaringan pada *link* instagram penambahan *follower.*

Pada simulasi penelitian ini dilakukan pembuatan *link phishing* pada kali linux yang merupakan *Operating System* yang *compatible. Link* ini merupakan bahan yang digunakan pelaku untuk melakukan penetrasi dalam mengambil akun korban. Selanjutnya dalam penelitian ini menggunakan OSCAR Method yang merupakan metode investigasi jaringan yang strategis dengan tahapan-tahapan yang dimiliki (Ahmad et al., 2021).

Dalam penyelidikan forensik jaringan pada Instagram, peneliti dapat memulai dengan menganalisis aliran data yang masuk dan keluar dari akun korban, termasuk aktivitas penambahan *follower* yang mencurigakan. Metode forensik yang umum digunakan dalam analisis jaringan Instagram adalah OSCAR. Selama proses forensik menggunakan metode OSCAR para peneliti dapat melacak sumber asal penambahan *follower* yang tidak wajar, mengevaluasi metode otentikasi yang mungkin telah diakses oleh pihak ketiga, dan mengidentifikasi aktivitas mencurigakan yang terkait dengan serangan *phishing*.

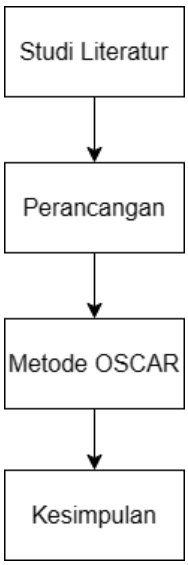
Hasil penelitian forensik ini dapat mencakup informasi tentang *IP address* dan *domain address* pelaku serta perilaku jaringan yang dapat membantu dalam penentuan asal serangan. Data yang diperoleh dari akses ini akan menjadi dasar analisis untuk mengidentifikasi bukti perundungan, yang nantinya dapat menjadi alat pendukung yang valid dalam proses pelaporan kepada pihak berwajib, sesuai dengan ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) (Pujianti, 2023).

2. METODE PENELITIAN

Menjelaskan kronologis penelitian, termasuk desain penelitian, prosedur penelitian (dalam bentuk algoritma, Pseudocode atau lainnya), bagaimana untuk menguji dan akuisisi data. Deskripsi dari program penelitian harus didukung referensi, sehingga penjelasan tersebut dapat diterima secara ilmiah. Jenis penelitian yang dilakukan yaitu penelitian kualitatif. penelitian kualitatif merupakan suatu teknik penelitian yang menggunakan narasi atau kata-kata dalam menjelaskan dan menjabarkan makna dari setiap fenomena, gejala, dan situasi sosial tertentu. Dalam penelitian kualitatif, peneliti adalah instrumen kunci untuk memaknai dan menginterpretasikan setiap fenomena, gejala dan situasi sosial tertentu (Waruwu, 2023). Penelitian ini berfokus terhadap penemuan bukti digital *phishing* pada jaringan yang digunakan korban dalam mengakses *link* pelaku menggunakan Metodologi OSCAR.

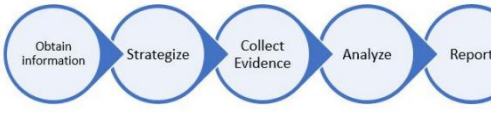
A. Desain Penelitian

Dalam penelitian ini digunakan model penelitian dengan dead forensics dengan kerangka kerja OSCAR. Terdapat 5 tahapan yang dilakukan peneliti yaitu studi literatur, perancangan, OSCAR Method, Kesimpulan.



Gambar 1 Desain Penelitian

a. Studi Literatur
   Melakukan tinjauan pustaka dalam memahami konsep dasar dead forensic, Metode OSCAR, Phishing, Forensic.
b. Perancangan
   Menyiapkan lingkungan penelitian untuk melakukan penelitian berupa menjalankan skenario yang telah gambarkan pada Gambar 3.
c. Metode OSCAR
   Penelitian ini menggunakan metode OSCAR untuk memastikan bahwa bukti forensik akurat. OSCAR merupakan akronim dari *Obtain information, Strategize, Collect evidence, Analyze, dan Report* (Davidoff & Ham, 2013).



Gambar 2 Metode OSCAR

- Tahap *obtain information*
  Obtain information yaitu tahap untuk memperoleh informasi tentang kejadian itu sendiri dan lingkungan di mana kejadian tersebut terjadi. Biasanya, informasi yang dikumpulkan tentang deskripsi kejadian, waktu, tanggal, dan bagaimana kejadian tersebut ditemukan. Informasi lain juga seperti sistem, orang, dan perangkat yang terlibat serta ringkasan tindakan yang diambil setelah penemuan kejadian.
- Tahap *Strategize*
  Strategize yaitu tahap pembuatan rencana rinci tentang bagaimana melakukan penyelidikan. Hal ini sebaiknya dilakukan dengan menggunakan berbagai kriteria, terutama karena bukti dari berbagai sumber memiliki tingkat volatilitas yang berbeda. Prioritas bukti sangat penting karena membantu penyelidik forensik menetapkan prioritas dalam penugasan personel dan sumber daya yang dibutuhkan dalam forensik jaringan.
- Tahap *Collect Evidence*
  Collect Evidence yaitu tahap perolehan dan prioritas sumber bukti. Bukti yang digunakan dalam forensik jaringan dapat diperoleh baik dari end devices maupun intermediate devices. Pada yang pertama, bukti dapat dikumpulkan dari perangkat milik penyerang atau korban, sedangkan pada yang kedua, bukti dapat diperoleh dari perangkat dan jaringan pihak ketiga. Selanjutnya adalah mengumpulkan bukti dari sumber yang diidentifikasi menggunakan prioritas yang telah ditetapkan.
- Tahap *Analyze*
  Analyze yaitu tahap menganalisa bukti-bukti yang sudah dikumpulkan. Hal-hal yang perlu diperhatikan dalam melakukan analisa yaitu korelasi bukti terhadap kejadian, timeline kejadian, kejadian-kejadian yang menarik, pemulihan bukti

tambahan, dan juga melakukan interpretasi.

- Tahap *Report*
  Report yaitu membuat laporan atas hasil perolehan hingga analisis. Laporan tersebut harus dapat dipahami oleh orang awam, deskriptif, dan faktual. Laporan dibuat dengan ringkas dengan tetap didukung detail yang dipertahankan.

d. Kesimpulan
Menarik kesimpulan dari apa yang telah dilakukan dalam penelitian.

B. Skenario

Skenario dalam penelitian ini disusun berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) [7] yang berisi mengatur bahwa orang perorangan termasuk yang melakukan kegiatan bisnis atau *e-commerce* di rumah dapat dikategorikan sebagai pengendali data pribadi sehingga untuk mengamankannya diperlukan UU. Skenario *phishing* yang akan disimulasikan pada penelitian ini berupa *phishing* penambahan *follower* Instagram.

Gambar 3 Skenario kasus phishing melalui Instagram

C. Tools

Pada penelitian ini diperlukan tools untuk mendukung penelitian. Tools ini terdiri dari hardware dan software. penggunaan tools dapat dilihat pada deskripsi tabel (1) berikut.

Tabel 1 Alat dan Bahan

No	Tools	Version
1	VM Kali Attack	2023.3
2	VM Kali Victim	2023.3
3	Instagram	-
4	GNS3 Virtual Switch	-
5	Zphisher	2.3.5
6	Wireshark	4.0.8

Berdasarkan tabel 1, objek utama dalam penelitian ini yaitu Kali victim yang telah mengakses *link phishing* pelaku. Zphisher digunakan dalam pembuatan link *phishing* (Rayat, 2023). Wireshark mendukung pelaksanaan penemuan bukti digital *phishing* dengan melihat log yang ada (Wireshark Foundation, 2016).

3. HASIL DAN PEMBAHASAN

Analisis *web phishing* dilakukan menggunakan metode yang telah dicantumkan pada skenario yaitu metode OSCAR.

a. *Obtain Information* (O)
Pada tahap ini dilakukan pengumpulan informasi terkait dengan insiden yang terjadi, dimana informasi ini akan digunakan peneliti untuk melakukan investigasi mendalam.

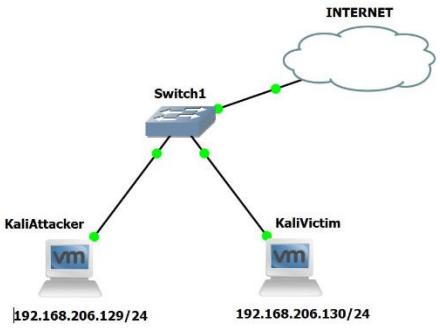
1. Informasi insiden
Berikut merupakan informasi yang didapat:

Tabel 2 Informasi Insiden

Informasi	Keterangan
Kasus Insiden	Terjadinya insiden web *phishing* yang dilakukan korban dengan imbalan followers instagram gratis. Penyerang berhasil mencuri *credential* korban dan mendapatkan username dan password.
Waktu insiden	Belum diketahui
Orang yang terlibat	Korban yang ingin menambah follower instagram

Tujuan serangan	Mendapatkan admin kredensial dan pengambilalihan akun pengguna

2. Informasi lingkungan
Informasi yang didapatkan peneliti berupa data yang telah diambil dari hasil skenario yang sudah disiapkan peneliti. Berikut topologi yang digunakan peneliti untuk menyiapkan skenario



Gambar 4. Topologi jaringan

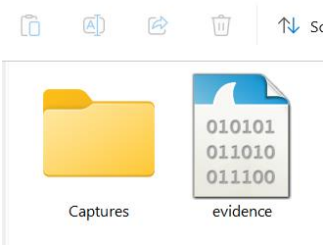
b. *Strategize*
Pada tahap pembuatan rencana rinci tentang bagaimana melakukan penyelidikan. Volatilitas bukti memiliki kriteria yang berbeda-beda sehingga dilakukan prioritas utama. Tahap ini dilakukan penentuan skala prioritas dari bukti digital yang diperoleh. Bukti digital yang diperoleh peneliti sebagai berikut,

Tabel 3 Strategize

Source of evidence	Effort	Volatility	Priority
Gambar topologi jaringan	Low	Low	3
Data paket jaringan	Medium	High	1
Link phishing	Medium	Medium	2

Ketiga evidence tersebut akan digunakan dalam tahap *Evidence Collection* untuk selanjutnya dianalisis sesuai dengan kegunaannya.

c. *Evidence Collection*
Evidence Collection merupakan tahapan dimana dilakukan pengumpulan bukti digital dari sumber bukti di tahap *Strategize.* Pada tahap ini dilakukan capture pada lalu lintas jaringan yang menghasilkan file PCAP data jaringan melalui capture Wireshark.



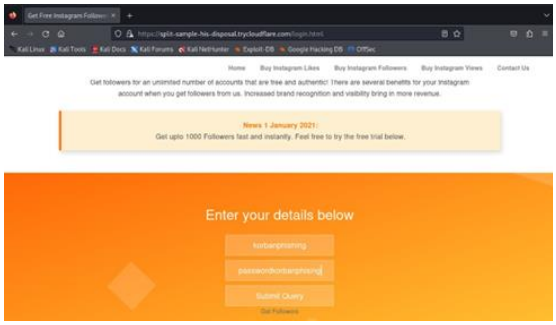
Gambar 5. File PCAP

Selain itu dilakukan pencatatan tanggal, waktu, sumber, dan nama penyelidik..

Tabel 3. Dokumen Bukti Phishing

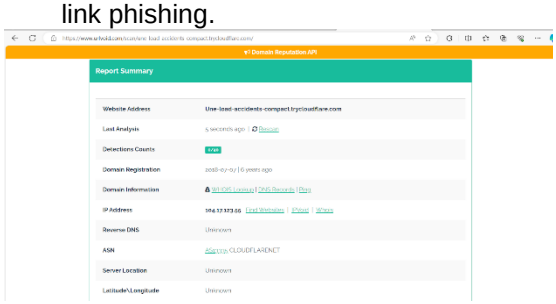
No	Catatan	Keterangan
1.	Tanggal	19 Desember 2023
2.	Waktu	23.01
3.	Sumber	Data jaringan
4.	Nama Penyelidik	R.M. Genggam, Dika A., Rahdian Ega

d. *Analyze*
Dari tahap sebelumnya telah didapatkan berbagai bukti terkait dengan tindak kejahatan Phishing. Tahap *analyze* ini dilakukan penganalisisan terhadap barang bukti menggunakan kali.
Analisis dimulai dari pengujian link phishing pelaku. Berikut merupakan link yang disebarkan penyerang dengan imbalan penambahan Followers Instagram secara gratis.



Gambar 6. Link Phishing

Penyelidik menggunakan link phishing tersebut kemudian melakukan analisis menggunakan tools URL void da terbukti merupakan link phishing.



Gambar 7. Link check URL

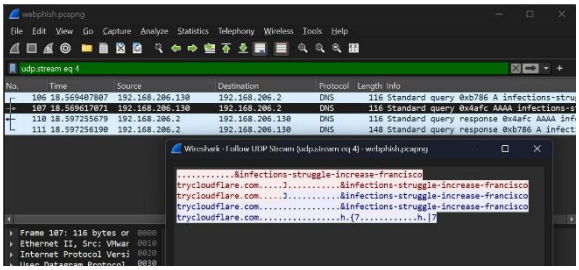
Selanjutnya dilakukan analisis terhadap link tersebut menggunakan tools Zphisher. Penyidik mensimulasikan bahwa ketika korban masuk ke dalam link phishing, penyerang dapat melihat akun kredensial korban berupa nama akun dan password dari korban.

Gambar 8. Kredensial korban

Selain itu, penyerang berhasil mendapatkan IP Address dari korban.

Gambar 9. IP Address korban

Pada langkah selanjutnya, peneliti melakukan analisis terhadap file *capture* menggunakan wireshark. File tersebut dianalisis terhadap data jaringan yang tercapture.



Gambar 10. Domain phishing

Dapat dilihat pada wireshark, penyidik menemukan domain *url phishing* yang diklik dan diakses oleh korban. Domain tersebut yaitu

split-sample-his-disposal.trycloudflare.com

Domain ini merupakan domain *Phishing* yang telah dibuat pelaku sehingga mendapatkan akses kredensial korban dan mengukuisisi Instagram korban.

e. Report

Pada tahap sebelumnya, telah diuraikan bahwa serangan phishing telah terjadi dengan tawaran peningkatan jumlah pengikut. Penyerang berhasil mendapatkan kredensial akun, bahkan mengambil alih kendali, dan kemudian memanfaatkannya untuk menyebarkan konten ilegal melalui akun Instagram korban. Tahap dari proses ini melibatkan pembuatan dokumen laporan yang vital bagi pemahaman publik yang lebih luas, termasuk pihak non-teknis seperti tim hukum, manajer, dan bahkan hakim. Dokumen ini dirancang agar mudah dipahami oleh orang-orang di luar lingkaran teknis, memberikan wawasan yang diperlukan untuk keperluan persidangan atau kebutuhan hukum lainnya, menjadikannya sebuah alat yang berharga di dalam ruang lingkup hukum. Dengan demikian, proses pelaporan tidak hanya memfasilitasi pemahaman tentang serangan tersebut, tetapi juga memberikan dukungan substansial dalam upaya penegakan hukum.

4. KESIMPULAN

Pengaplikasian metode OSCAR yang dibantu dengan tools Wireshark dapat mengetahui penyebab mengapa korban mengalami kejahatan ini yaitu korban mengklik suatu laman atau pranala yang telah dibuat oleh pelaku kejahatan. Pengujian investigasi penyerangan web phishing pada studi kasus Instagram dilakukan dalam beberapa tahapan atau cara seperti Obtain information, Strategize, Collect evidence, Analyze, dan Report sesuai dengan metode yang telah diusulkan oleh OSCAR dengan tindak lanjut analisis barang bukti yang didapat. Dari hasil pengolahan data yang dianalisis didapatkan bahwa:

- Pelaku kejahatan menggunakan protokol https sebagai protokol untuk mengambil data atau file pada laman penipuan milik pelaku.
- Di dalam paket pengiriman yang dianalisis pelaku melakukan redirecting laman palsu miliknya ke laman asli milik Instagram untuk menghilangkan kecurigaan korban.
- Pelaku menggunakan IP Address cukup beragam yang bergantung pada siapa target yang ingin diincar oleh pelaku dan pelaku menggunakan hosting laman yang memiliki IP bersifat dinamis sehingga sulit untuk dilakukan pelacakan terkait tindak kejahatan tersebut.

DAFTAR PUSTAKA

A. Rizka Ramadhanta and N. Maghfirah Aesthetika, “Content Analysis of Instagram Social Media Accounts @3second Local Brand Fashion Products [Analisis Konten Akun Media Sosial Instagram @3second Produk Fashion Merek Lokal],” Aug. 2023.

Ahmad, N. A., Baharum, Z., Zainal, A., Razak, F. H. A., & Adnan, W. A. W. (2021). Spiritual User Experience (iSUX) for Older Adult Users using Mobile Application. *International Journal of Advanced Computer Science and Applications*, *12*(5). https://doi.org/10.14569/ijacsa.2021.0120510

Arshad, H., Jantan, A., Hoon, G. K., & Abiodun, I. O. (2020). Formal knowledge model for online social network forensics. *Computers & Security*, *89*, 101675. https://doi.org/10.1016/j.cose.2019.101675

Davidoff, S., & Ham, J. (2013). *Network Forensics*. https://ptgmedia.pearsoncmg.com/images/9780132564717/samplepages/0132564718.pdf

Parker, H. J., & Flowerday, S. V. (2020). Contributing factors to increased susceptibility to social media phishing attacks. *SA Journal of Information Management*, *22*(1). https://doi.org/10.4102/sajim.v22i1.1176

Pujianti, S. (2023, February 13). *Pemerintah: UU Perlindungan Data Pribadi Beri Perlindungan Hukum | Mahkamah Konstitusi Republik Indonesia*. Www.mkri.id. https://www.mkri.id/index.php?page=web.Berita&id=18915

Rayat, T. (2023, December 20). *Build software better, together*. GitHub. https://github.com/topics/zphisher

Shaw, U., Das, D., & Medhi, S. (2016). Social Network Forensics: Survey and Challenges. *International Journal of Computer Science and Information Security,*.

Waruwu, M. (2023). Pendekatan Penelitian Pendidikan: Metode Penelitian Kualitatif, Metode Penelitian Kuantitatif dan Metode Penelitian Kombinasi (Mixed Method). *Jurnal Pendidikan Tambusai*, *7*(1), 2896–2910. https://doi.org/10.31004/jptam.v7i1.6187

Widi, S. (2023, February 3). Pengguna Media Sosial di Indonesia Sebanyak 167 Juta pada 2023. Dataindonesia.id. https://dataindonesia.id/internet/detail/pengguna-media-sosial-di-indonesia-sebanyak-167-juta-pada-2023

Wireshark Foundation. (2016). *Wireshark*. Wireshark.org. https://www.wireshark.org/