Analisis Digital Forensik Spear Phishing Menggunakan Metode National Institute of Justice (Studi Kasus: Instagram Verified Account)

Aris Dwi Prasetyo[1], Henki Bayu Seta[2], I Wayan Widi P.[3]
[1,2,3] Fakultas Ilmu Komputer
[1,2,3] Universitas Pembangunan Nasional Veteran Jakarta
[1,2,3] Jl. RS Fatmawati No. 1, Pondok Labu, Jakarta Selatan DKI Jakarta 12450
arisdwi@upnvj.ac.id[1], henkiseta@upnvj.ac.id[2], wayan.widi@upnvj.ac.id[3]

Abstrak. Media sosial memudahkan interaksi antar pengguna sebagai alat penyebaran informasi. Sehingga semua orang mencoba untuk memperoleh seluruh atensi yang ada pada suatu platform seperti Instagram. Hal ini menimbulkan dampak negatif seperti penipuan akun, pencurian data pribadi, dan penjualan akun yang telah diretas. Jenis kejahatan yang sering terjadi adalah Phishing yaitu penipuan yang menampilkan hal yang sama persis dengan platform yang asli. Digital forensik dapat memudahkan pencarian barang bukti digital. Dalam penelitian ini peneliti akan melakukan analisis digital forensik terkait tindak kejahatan spear phishing dengan menggunakan metode yang telah diusulkan oleh National Institute of Justice (NIJ). Dalam metode ini tahapan yang akan dilakukan antara lain Preparation, Collection, Examination, Analysis, dan Reporting. Berdasarkan penelitian didapatkan laman phishing yang digunakan oleh pelaku dengan domain laman instagram-page-login.herokuapp.com dan IP Address yang digunakan yaitu 18.208.60.216 dan 54.165.58.209.

Kata Kunci: Digital Forensik, *Spear Phishing*, Instagram, *National Institute of Justice*.

1 Pendahuluan

Perkembangan media sosial memudahkan interaksi antar pengguna internet. Media sosial memiliki peran penting sebagai alat penyebaran informasi mengenai seseorang maupun suatu brand yang ada. Sehingga semua orang mencoba untuk memperoleh seluruh atensi yang ada pada suatu platform seperti Instagram. Instagram membatasi para influencer dengan memberikan tanda verifikasi pada akun influencer. Namun perkembangan media sosial memiliki dampak negatif seperti penipuan akun, pencurian data pribadi, dan penjualan akun yang telah diretas oleh peretas atau hacker. Jenis kejahatan yang sering terjadi adalah Phishing yaitu penipuan yang seolah menampilkan keorisinilan dan keamanan data yang seharusnya dilakukan dalam suatu jaringan internet.

Pada tahun 2021 setidaknya terjadi 264 kasus phishing yang berhasil dicatat oleh BSSN Indonesia. Berdasarkan data tahunan BSSN phishing dibagi menjadi 5 jenis, yaitu: Email Phishing, Spear Phishing, Whaling, Vishing, dan Smishing. Kejahatan ini dapat menimbulkan kerugian yang nyata karena data korban dapat digunakan untuk melakukan tindakan negatif seperti mencuri dengan mengatasnamakan korban, meretas sistem komputer, hingga tindakan lainnya yang merugikan dari sisi keamanan.

Digital forensik memudahkan pencarian informasi penting terkait barang bukti digital yang akan memberatkan maupun melemahkan pidana yang hendak dijatuhkan dalam suatu kasus kejahatan. Metode yang dapat digunakan dalam ilmu digital forensik telah diusulkan oleh National Institute of Justice (NIJ). Dalam memudahkan investigasi terkait kasus kejahatan dan pelaku, diperlukan pengolahan data yang telah dicapture untuk pelacakan berdasarkan IP address dan DNS pelaku.

2 Tinjauan Pustaka

2.1 Identifikasi Masalah

Spear phishing merupakan teknik menargetkan individu atau suatu kelompok tertentu [1]. Spear phishing marak terjadi di kalangan influencer media sosial. Peretas akan mengirimkan sebuah surel yang terlihat dikirimkan oleh sebuah organisasi yang terkenal bagi korban [2]. Surel tersebut dapat berisi sebuah tautan yang dapat menarik perhatian korban untuk mengklik pranala terkait dan memulai pengunduhan program berbahaya, atau memaksa korban untuk memasukkan informasi pribadi ke situs jejaring palsu yang memiliki tampilan menyerupai halaman jejaring orisinal [3].

2.2 Digital Forensik

Digital Forensik merupakan cabang ilmu teknologi dan kriminologi yang memudahkan penyidik guna menelusuri barang bukti digital untuk pembuktian hukum [4]. Digital Forensik mencakup pemulihan barang bukti dan melakukan penyidikan lebih lanjut pada perangkat, jaringan internet, dan aplikasi yang menjadi barang bukti digital [5]. Forensik dilakukan dimana barang bukti dianalisis dalam keadaan perangkat korban ataupun pelaku dalam keadaan menyala untuk mencari bukti-bukti kejahatan yang masih tersimpan secara volatil [6].

2.3 *National Institute of Justice* (NIJ)

National Institute of Justice (NIJ) merupakan sebuah organisasi departemen kehakiman Amerika Serikat. NIJ berfokus dalam penelitian, pengembangan, dan evaluasi terkait masalah pengendalian kejahatan. NIJ mempublikasikan penelitian yang membantu dalam proses pengolahan barang bukti kejahatan yang digunakan oleh spesialis maupun penyidik. Terdapat 5 tahapan dalam metode yang diusulkan oleh *National Institute of Justice* (NIJ) yang akan digunakan dalam analisis barang bukti. Adapun kelima tahapannya seperti:

a) Persiapan (*Preparation*)

Tahapan menyiapkan peralatan yang akan digunakan untuk keperluan penyelidikan dalam upaya menguak seluruh barang bukti yang ada. peralatan yang akan digunakan selama proses pengolahan barang bukti sesuai anjuran dalam keilmuan digital forensik, yaitu aplikasi *Wireshark, NetworkMiner, Hashcalc,* dan *WHOIS* sebagai peranti lunak untuk pemrosesan barang bukti.

b) Pengumpulan (*Collection*)

Tahapan pencarian barang bukti yang ada melalui pengumpulan seluruh data dengan cara menduplikasi ruang penyimpanan perangkat terkait. Barang bukti yang didapatkan dari perangkat korban maupun pelaku yang mana hasilnya akan berupa lalu lintas jaringan yang terjadi dalam satu kasus kejahatan dengan ekstensi .pcap yang nantinya dapat digunakan dengan aplikasi *Network Analyzer* seperti *Wireshark* dan *NetworkMiner*.

c) Pengujian (*Examination*)

Tahapan pemeriksaan barang bukti terkait untuk memeriksa keseluruhan barang sudah diduplikasi dengan sempurna berdasarkan md5 dan *hash file* yang ada.

d) Penyelidikan (*Analysis*)

Tahapan penganalisisan barang bukti duplikasi secara mendetail dengan cara yang diusulkan sesuai hukum yang berlaku untuk menemukan bukti otentik kejahatan yang telah terjadi. Analisis akan lebih memfokuskan untuk mendapatkan informasi terkait:

- Bagaimana kejahatan tersebut dapat terjadi?
- Kapan kasus kejahatan tersebut terjadi?
- Pranala atau link mana yang digunakan penjahat untuk menipu korban?
- IP dan DNS manakah yang digunakan Pelaku untuk menipu korban?

e) Pelaporan (*Reporting*)

Tahapan akhir pelaporan barang bukti kejahatan yang telah ditemukan saat tahap penyelidikan, penjelasan mengenai peralatan yang digunakan selama proses pengolahan barang bukti, metode yang digunakan untuk mengolah barang bukti, dan saran dalam upaya evaluasi barang bukti tindak kejahatan.

2.4 *Wireshark*

Wireshark merupakan seperangkat alat yang digunakan dalam penyelidikan transfer data yang telah terjadi di dalam suatu jejaring internet, peranti lunak yang digunakan memiliki peralatan yang berfungsi dalam pelacakan data sehingga memudahkan penyidik dalam menganalisis pertukaran data yang terjadi pada suatu jaringan [7].

2.5 *NetworkMiner*

NetworkMiner merupakan alat analisis forensik jaringan yang dapat digunakan sebagai penangkap lalu lintas jaringan dalam suatu jejaring internet, peranti lunak yang digunakan memiliki peralatan yang berfungsi dalam pemetaan *session* yang terjadi, *host* yang terhubung, dan informasi yang terdapat dalam suatu jaringan.

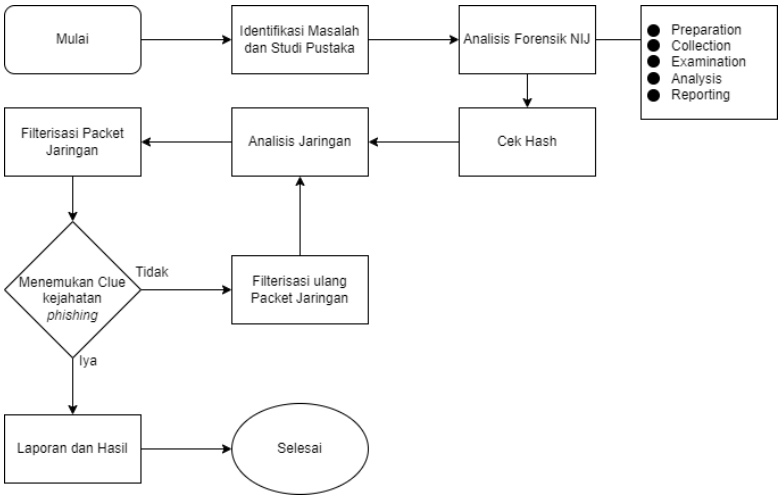
2.6 Pemetaan Jaringan (*Network Addressing*)

Pemetaan Jaringan merupakan sebuah teknik yang digunakan untuk mengetahui darimana sumber sebuah paket jaringan dikirimkan, dalam penelitian ini peneliti menggunakan alamat *IP (IP Address)*, yaitu sebuah alamat virtual yang sudah diterapkan di seluruh perangkat yang terhubung ke dalam suatu jaringan yang menggunakan *Internet Protocol* tertentu. Penentuan alamat *IP* ini bersifat dinamis yang mana dapat berubah sesuai konfigurasi pada *DHCP* yang digunakan.

2.7 Evaluasi

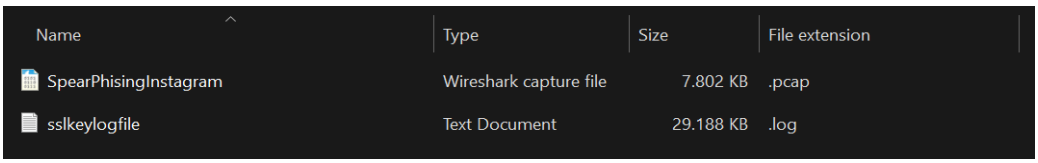
Barang bukti yang sudah didapat dari proses analisis menggunakan metode National Institute of Justice (NIJ) akan dianalisis lebih lanjut untuk mengetahui informasi lebih mendetail terkait pelaku. Aplikasi yang digunakan merupakan WHOIS dan Central OPS.

3 Hasil



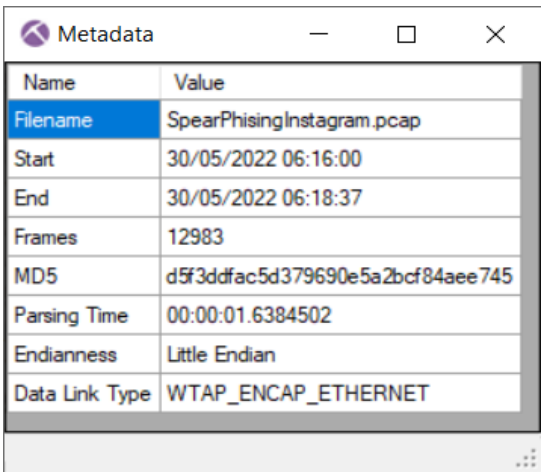
Gambar. 1. Flowchart Penelitian

Data yang digunakan untuk melakukan penelitian ini didapatkan dari hasil *capture* menggunakan aplikasi *Wireshark* terhadap jaringan nirkabel area publik. Dimana data *capture* yang dibutuhkan akan digunakan sesuai pedoman yang diusulkan oleh *National Institute of Justice* yaitu: data akan diakuisisi dari perangkat secara langsung yang nantinya akan dilakukan pengujian menggunakan aplikasi yang memiliki fitur pengecekan nilai hash.



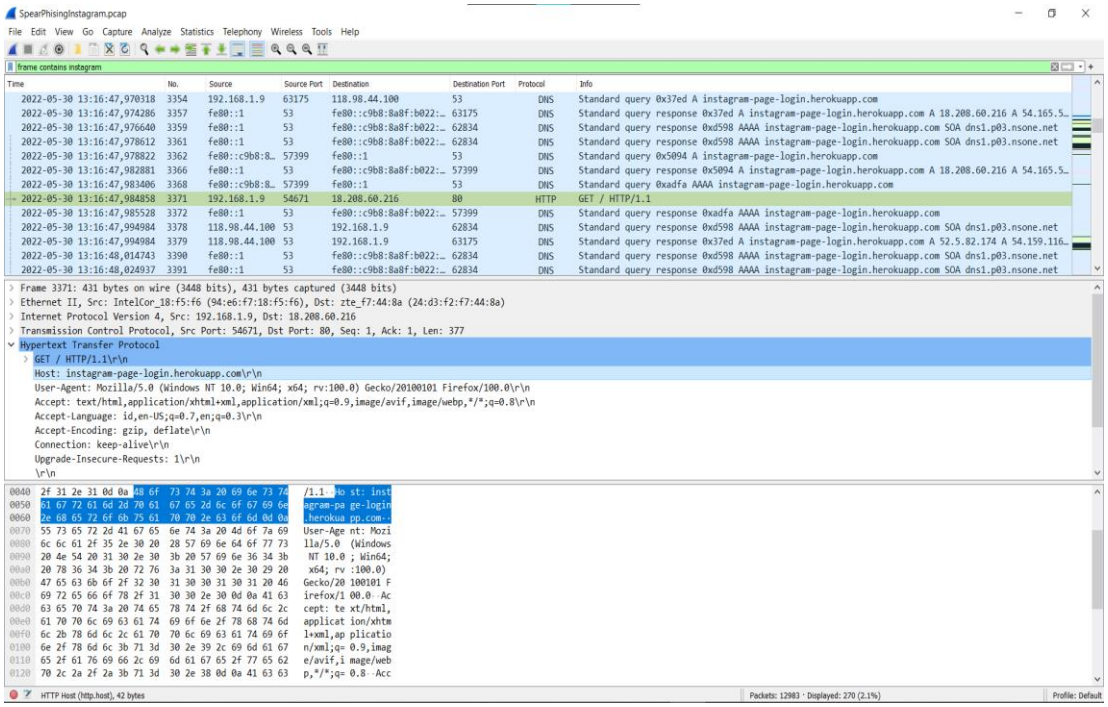
Gambar. 2. Barang bukti tindak kejahatan phishing *Instagram*

Pada Gambar. 2 merupakan tampilan file barang bukti yang digunakan dalam penelitian. File tersebut memiliki ekstensi (.pcap) yang nantinya akan dianalisis menggunakan aplikasi *network analyzer* seperti *Wireshark* maupun *NetworkMiner*. Untuk menunjang pen*decrypt*-an paket jaringan maka akan digunakan *sslkeylogfile* yang ada dan dapat dimanfaatkan menggunakan fitur yang disediakan oleh aplikasi *Wireshark*.



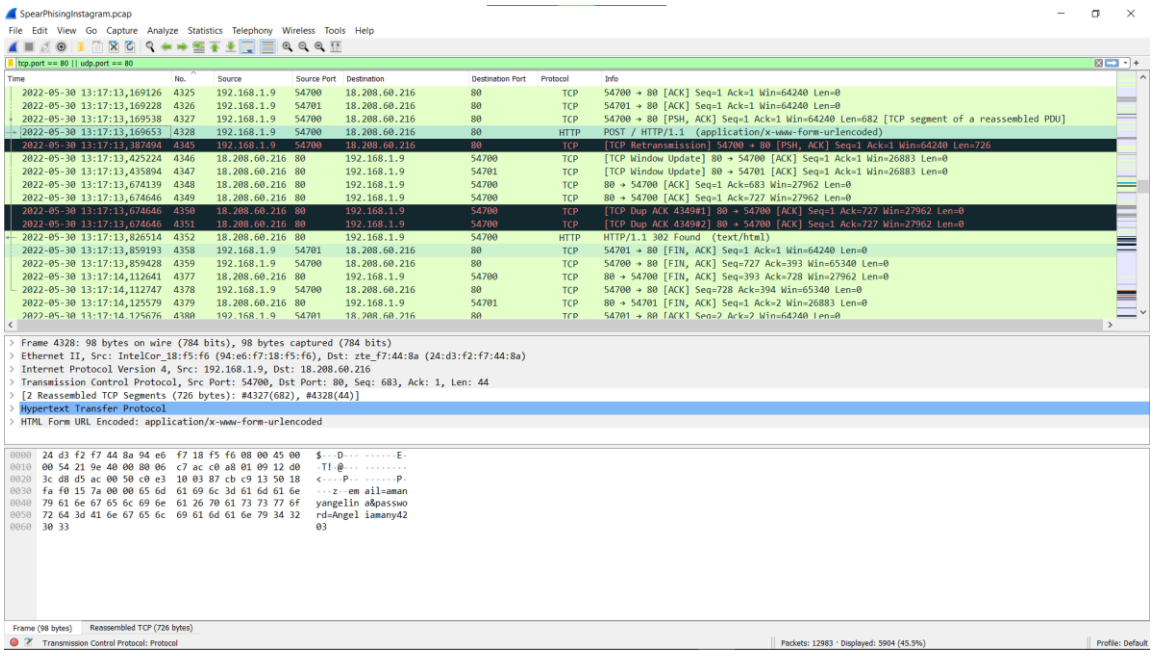
Gambar. 3. Informasi detail terkait md5 yang ada pada file barang bukti

Pada Gambar. 3 didapatkan informasi mendetail terkait barang bukti yang digunakan dalam penelitian. yaitu barang bukti tersebut memiliki rentang waktu paket dalam jaringan yang berjalan pada tanggal 30 bulan Mei tahun 2022 pada pukul 06.16.00 hingga 06.18.37 dalam standar waktu UTC. Informasi lain yang didapatkan dari penggunaan aplikasi ini adalah nilai hash yang ada pada barang bukti yang digunakan, barang bukti tersebut menggunakan algoritma MD5 dengan nilai hash d5f3ddfac5d379690e5a2bcf84aee745. Barang bukti tersebut juga memiliki sejumlah 12983 *Frame* secara total.



Gambar. 4. Filterisasi "*frame contains Instagram*"

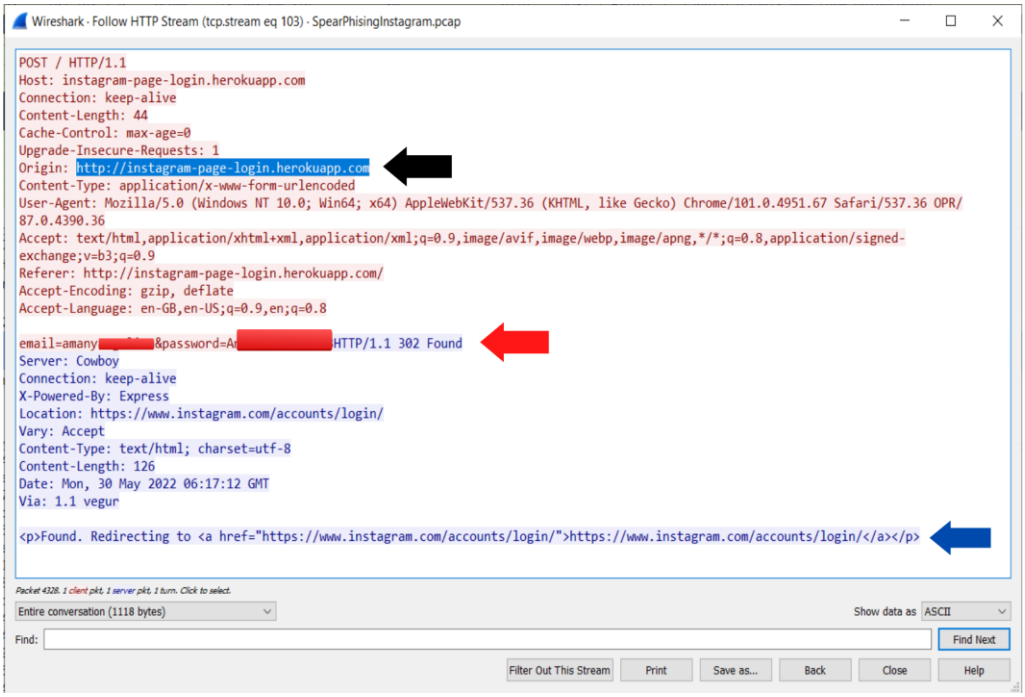
Pada Gambar. 4 menampilkan penggunaan filterisasi untuk memilah paket data yang berhubungan langsung dengan *Instagram*. Hal ini dilakukan karena target penyerangan *phishing* berfokus dalam memancing korbannya untuk memverifikasi akun *Instagram* mereka ke laman *phishing* yang telah dibuat oleh pelaku kejahatan Salah satu paket data meminta perintah GET terhadap IP *address* 18.200.60.216 yang mengarah pada sebuat *website* yang *dihost* oleh laman dengan nama "*instagram-page-login.herokuapp.com*".



Gambar. 5. Filterisasi *"tcp.port == 80 || udp.port == 80"*

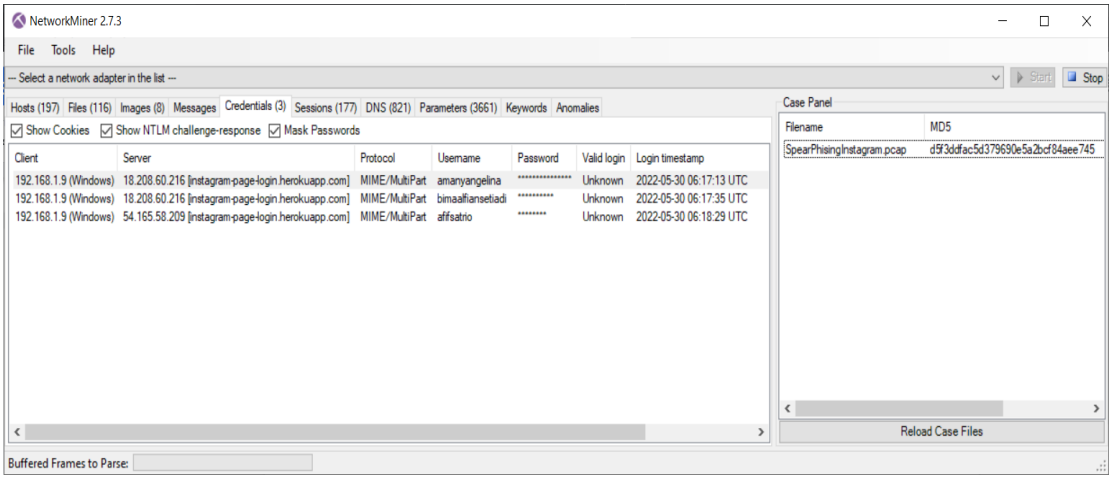
ISSN: 2655-139X (ONLINE)
ISSN: 0216-4221 (PRINT)

Pada Gambar. 5 menunjukkan temuan port yang digunakan yaitu port 80 baik *TCP* maupun *UDP* terdapat metode POST dalam transaksi jaringan tersebut. Hal ini membuktikan korban berhasil memasukkan data kredensial akun Instagram ke dalam laman yang tidak memiliki keabsahan apapun terkait *Instagram*. Lalu *log* tersebut ditelusuri menggunakan fitur *Follow TCP Stream Wireshark* yang menunjukkan data lebih lengkap terkait proses perpindahan data ini.



Gambar. 6. *Follow TCP Stream Wireshark*

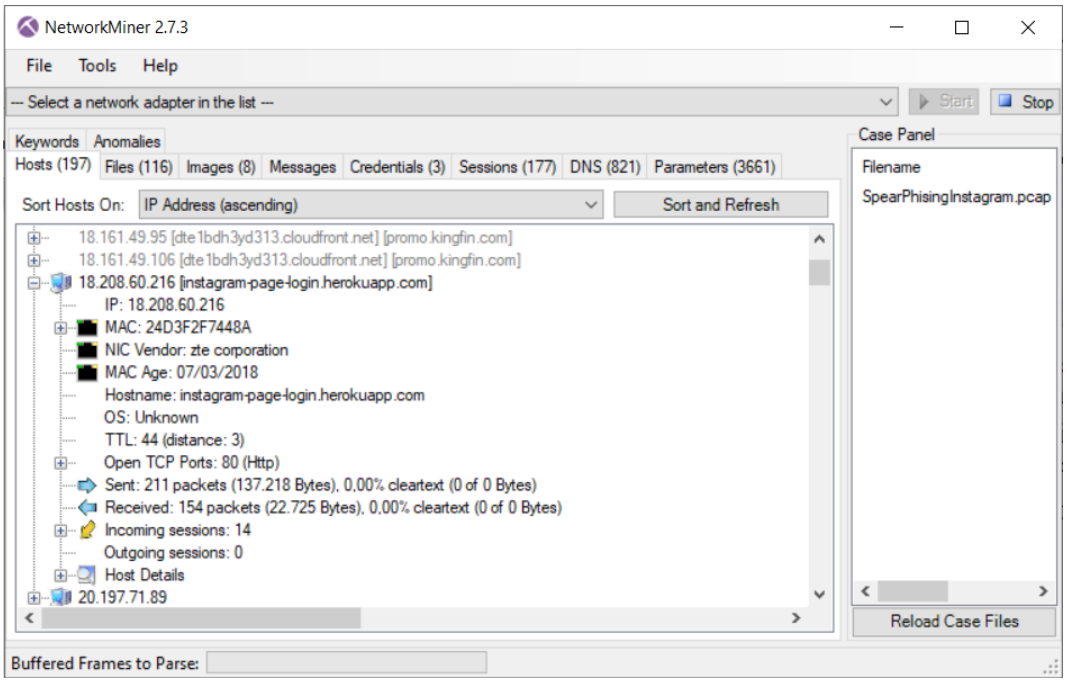
Pada Gambar. 6 didapatkan informasi mendetail terkait proses pengiriman data kredensial yang telah terjadi. Korban mengisi data kredensial tersebut pada laman "*http://instagram-page-login.herokuapp.com*", setelah korban memasukkan data kredensial maka pelaku akan mendapatkan salinan data yang dimasukkan oleh korban pada *database* yang telah pelaku siapkan. Untuk menghilangkan jejak. Pelaku melakukan proses *redirecting* laman menuju laman asli *Instagram* yang membuat korban tidak curiga dan hanya perlu mengisi ulang data kredensial pada laman asli *Instagram*.



Gambar. 7. Informasi Data Kredensial pada Aplikasi *NetworkMiner*

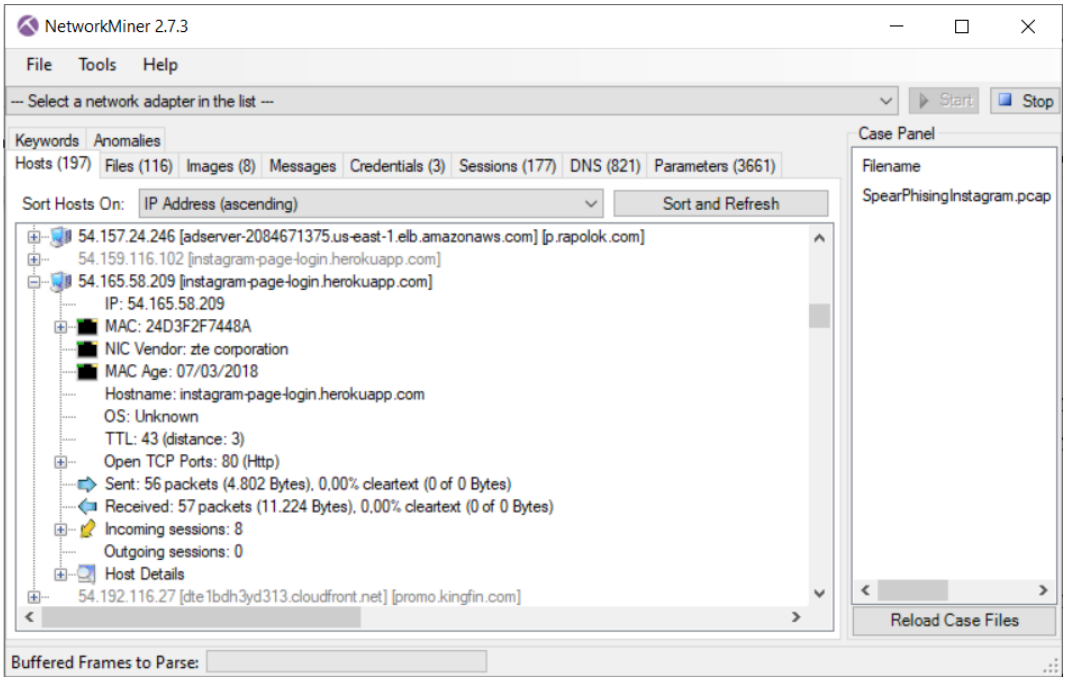
Penggunaan aplikasi *NetworkMiner* pada Gambar 7 menunjukkan Informasi terkait data kredensial yang berhasil di*capture*. Terdapat tiga korban yang semuanya memasukkan informasi kredensial pada Server yang dimiliki oleh [instagram-page-login.herokuapp.com] baik melalui IP 18.208.60.216 maupun 54.165.58.209. memiliki *timestamp* yang terjadi pada tanggal 30 bulan Mei tahun 2022 dengan format waktu UTC. Informasi

kredensial yang didapat menggunakan aplikasi *NetworkMiner* sesuai dengan data yang didapat dari aktivitas *Follow TCP Stream* pada aplikasi *Wireshark*.



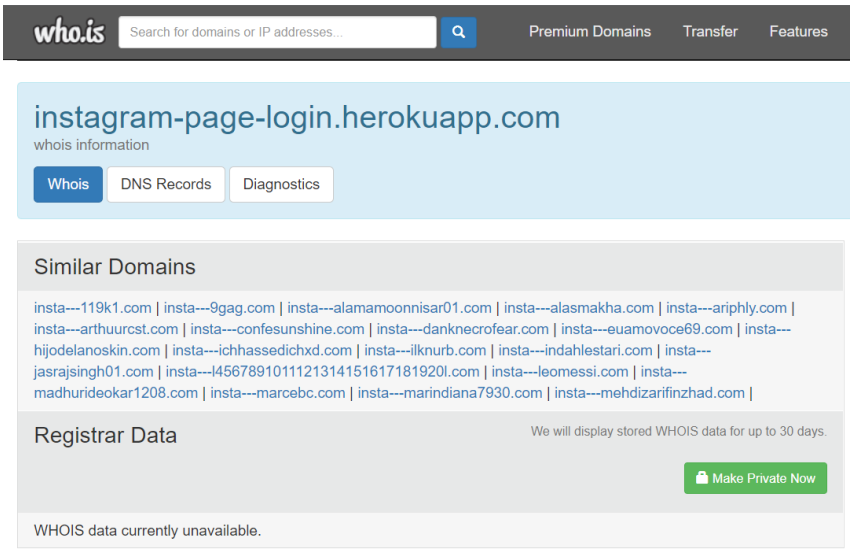
Gambar. 8. *IP Address 18.208.60.216*

Pada Gambar 8 menampilkan *IP Address* 18.208.60.216 memiliki transaksi pengiriman sejumlah 211 Paket (137.218 *Bytes*) dan transaksi penerimaan sebanyak 154 Paket (22.725 *Bytes*) dan dilakukan dalam 14 *Sessions* keseluruhannya menggunakan *port 80* dan menuju *host* yang sama yaitu [instagram-page-login.herokuapp.com].



Gambar. 9. *IP Address 54.165.58.209*

Pada Gambar 9 menampilkan *IP Address* 54.165.58.209 yang terlampir pada Gambar 4.21 menunjukkan terdapat transaksi pengiriman sejumlah 56 Paket (4.802 *Bytes*) dan transaksi penerimaan sebanyak 57 Paket (11.224 *Bytes*) dan dilakukan dalam 8 Sessions keseluruhannya menggunakan *port 80* dan menuju *host* yang sama yaitu [instagram-page-login.herokuapp.com].

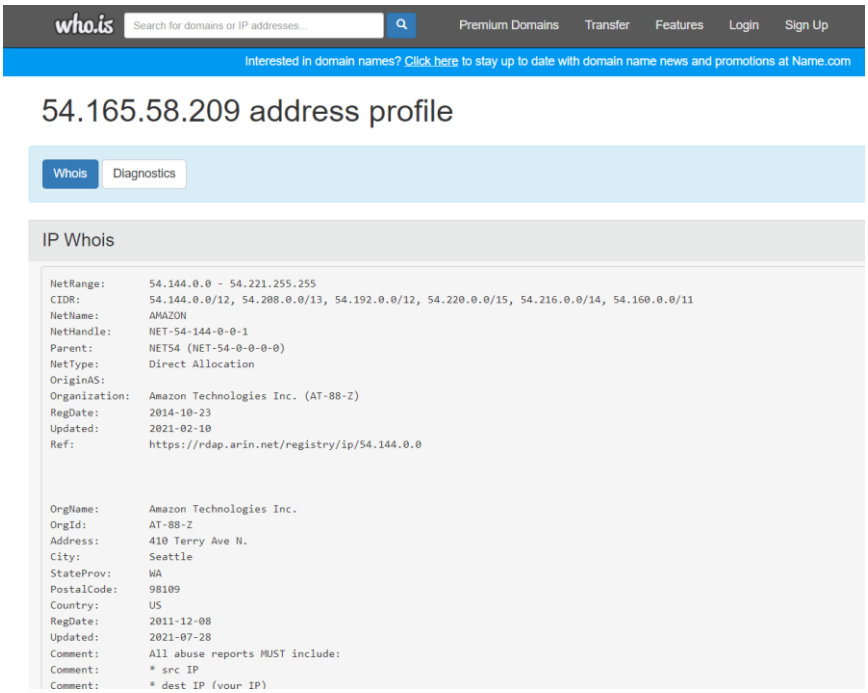


Gambar. 10. Analisis *WHO.is* pada *Domain*

Berdasarkan analisis yang dilakukan pada Gambar 10, laman [instagram-page-login.herokuapp.com] masih belum didaftarkan pada *database* yang tersedia pada aplikasi *WHOis* maupun *Central OPS* sehingga diperlukan pencarian yang mengarah ke hal yang lebih umum, yaitu pencarian menggunakan *IP Address* dan *Domain* dimana laman tersebut di*hosting*.

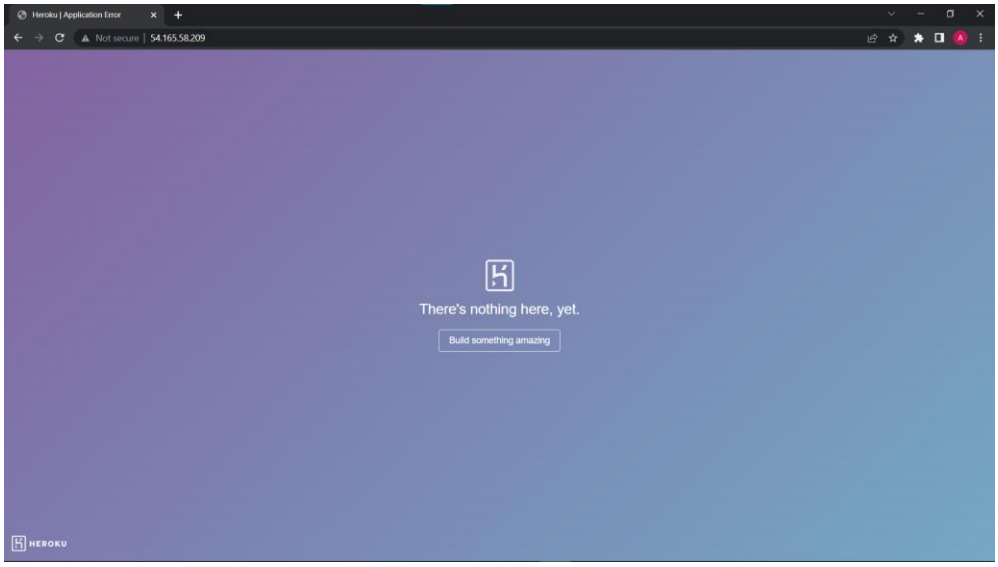
Gambar. 11. Analisis *IP Address WHO.is 1*

Pada Gambar 11, pencarian informasi berdasarkan *IP Address* 18.208.60.216 menggunakan aplikasi *WHO.is* yaitu penyedia *IP address* tersebut merupakan perusahaan *Amazon Technologies Inc* yang menyediakan IP yang bersifat *dynamic* dengan *range* 18.32.0.0 – 18.255.255.255. dimana lokasi perusahaan tersebut berada pada negara US dan berada pada kota Seattle namun tidak ada informasi terkait pelaku tindak kejahatan.



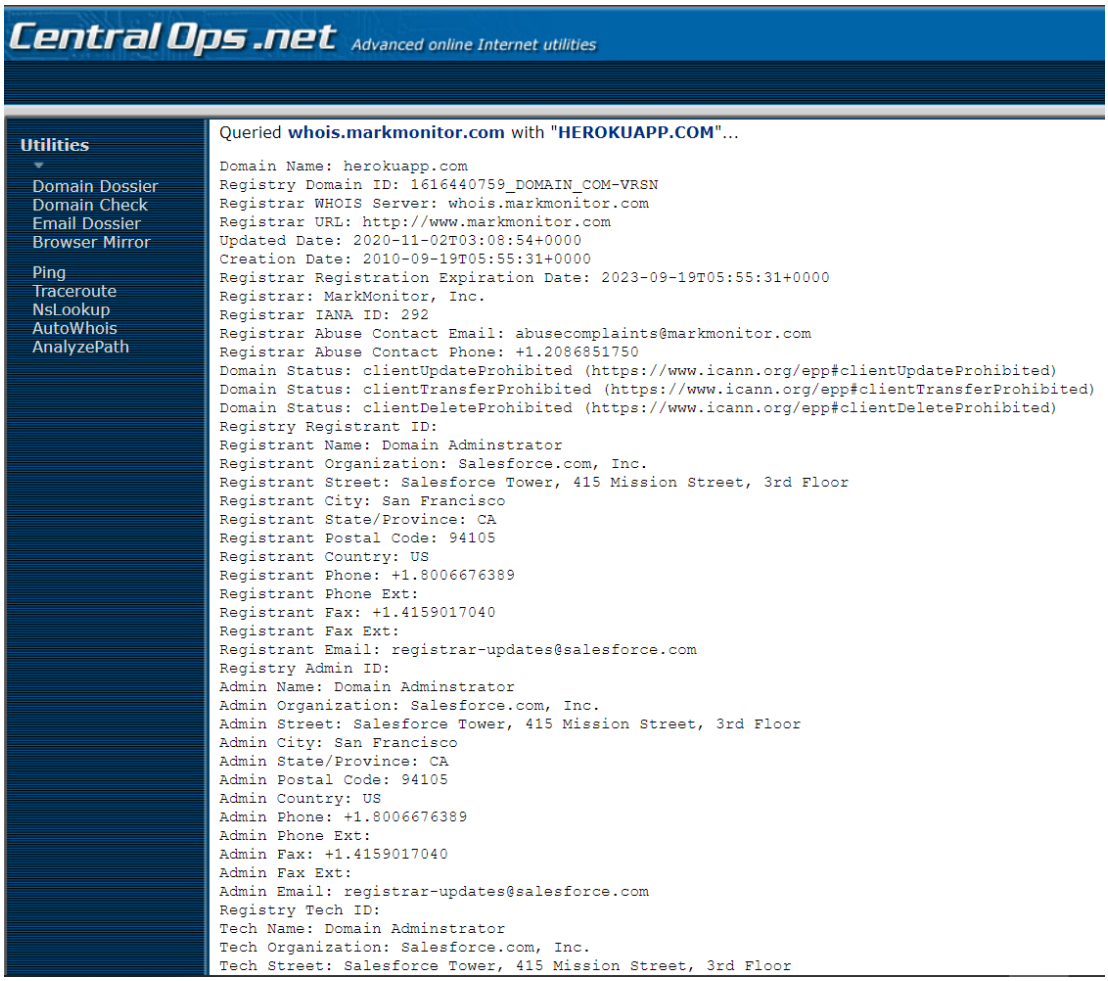
Gambar. 12. Analisis *IP Address WHO.is 2*

Pencarian berikutnya pada Gambar 12 berdasarkan *IP Address* didapat informasi terkait *IP Address* 54.165.58.209 yaitu penyedia *IP address* tersebut merupakan perusahaan *Amazon Technologies Inc* yang menyediakan IP yang bersifat *dynamic* dengan range 54.144.0.0 - 54.221.255.255. dimana lokasi perusahaan tersebut berada pada negara US dan berada pada kota Seattle namun tidak ada informasi terkait pelaku tindak kejahatan.



Gambar. 13. *Cross-check IP Address*

Pada Gambar 13 menunjukkan pencarian berdasarkan *IP Address* yang digunakan oleh pelaku dalam tindak kejahatan tersebut tidak dapat menunjukkan hasil yang mengarah pada individu tertentu diakibatkan oleh pelaku yang menggunakan *IP Address* yang bersifat *dynamic*.



Gambar. 14. Analisis *Hosting Heroku*

Pada Gambar 14 menunjukkan berdasarkan *domain hosting* yang digunakan yaitu *Herokuapp.com* didapatkan beberapa informasi terkait nama *domain* yang digunakan yaitu HEROKUAPP.COM, lisensi pendaftaran WHOIS, Nama *server* yang digunakan, dan informasi kontak terkait pelaporan data yang dianggap melanggar peraturan yang sudah diatur oleh pemilik perusahaan *markmonitor* seperti *abusecomplaints@markmonitor.com* dan nomor telepon penanggung jawab *hosting* pada nomor +1 2086851750.

Dapat disimpulkan bahwa pelaku menggunakan layanan yang disediakan oleh *Hosting* HEROKUAPP.COM untuk membuat laman web penipuan. Untuk mengetahui informasi lebih lanjut terkait pelaku kejahatan dibutuhkan izin pihak berwenang untuk menghubungi pihak yang meng*hosting* laman tersebut.

4 Kesimpulan dan Saran

4.1 Kesimpulan

1. Pengaplikasian metode NIJ yang dibantu dengan tools Wireshark dan NetworkMiner dapat mengetahui penyebab mengapa korban mengalami kejahatan ini dikarenakan korban mengklik suatu laman atau pranala yang telah dibuat oleh pelaku kejahatan.
2. Identitas pelaku kejahatan tidak berhasil didapatkan berdasarkan referensi dari Domain yang digunakan pelaku karena tidak terdaftar pada database Who.is maupun Central OPS, dan IP Address yang digunakan pelaku karena bersifat dinamis. Menggunakan domain yang terekam oleh tools Wireshark dan NetworkMiner menghasilkan informasi terkait perusahaan dimana pelaku melakukan hosting laman penipuan dalam tindak kejahatan tersebut.
3. Pengujian investigasi penyerangan spear phishing pada studi kasus Instagram dilakukan dalam beberapa tahapan atau cara seperti Preparation, Collection, Examination, Analysis, dan Reporting sesuai dengan

metode yang telah diusulkan oleh pihak National Institute of Justice (NIJ) dengan tindak lanjut analisis barang bukti yang didapat.

4. Dari hasil pengolahan data yang dianalisis didapatkan bahwa:
   - Pelaku kejahatan menggunakan protokol http sebagai protokol untuk mengambil data atau file pada laman penipuan milik pelaku. Maka dapat digunakan fitur filtrasi yang disediakan oleh aplikasi Wireshark berupa tcp.port == 80 || udp.port == 80 guna mempermudah analisis.
   - 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.

4.2 Saran

Penelitian selanjutnya diharapkan dapat menggunakan tools yang lebih memadai dalam pendekripsian lalu lintas jaringan. Melakukan proses capture data melalui suatu jaringan secara menyeluruh melalui berbagai device dan lebih memperdalam pengusutan pencarian informasi terkait pelaku tindak pidana.

Referensi

[1] A. E. Agazzi, “Phishing and Spear Phishing: examples in Cyber Espionage and techniques to protect against them,” May 2020, [Online]. Available: http://arxiv.org/abs/2006.00577

[2] M. H. Wibowo and N. Fatimah, “Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime,” vol.1, no.1, pp.1-5 ,2017. doi: 10.29100/.v1i1.69.g47.

[3] A. S. Y. Irawan, N. Heryana, H. S. Hopipah, and D. Rahma, “Identifikasi Website Phishing dengan Perbandingan Algoritma Klasifikasi”, *Syntax J. Inf.*, vol. 10, no.1, pp. 57–67, Jun. 2021.

[4] R. A. Kinasih, A. W. Muhammad, and W. A. Prabowo, “Analisis Keamanan Browser Menggunakan Metode National Institute of Justice (Studi Kasus: Facebook dan Instagram)”, *Digitalzone*, vol. 11, no. 2, pp. 174-184, Nov. 2020, doi: 10.31849/digitalzone.v11i2.4678ICCS.

[5] Mushlihudin and A. Nofiyan, “Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology,” *CYBERNETICS*, vol. 4, no. 02, pp. 79–92, 2020, [Online]. Available: https://centralops.net

[6] R. Umar, I. Riadi, and B. F. Muthohirin, “Live forensics of tools on android devices for email forensics,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 4, pp. 1803–1809, Aug. 2019, doi: 10.12928/TELKOMNIKA.v17i4.11748.

[7] R. Hanipah and H. Dhika, “Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark,” *Journal of Computer and Information Technology*, vol.4, no.1, pp.11-23, 2020, doi: http://doi.org/10.25273/doubleclick.v4i1.5668