Analisis Serangan *Web Phishing* pada Layanan *E-commerce* dengan Metode *Network Forensic Process*

Aseh Ginanjar[1], Nur Widiyasono[2], Rohmat Gunawan[3]
Program Studi Informatika, Universitas Siliwangi
Jl. Siliwangi No.24 Kota Tasikmalaya 46115
[1]*147006150@student.unsil.ac.id*
[2]*nur.widiyasono@unsil.ac.id*
[3]*rohmatgunawan@unsil.ac.id*

Abstract*—*E-commerce provides facilities to reach customers around the world without geographical market restrictions. As a result, the number of customers who depend on the internet for purchases has experienced a significant increase. The potential for cybercrime attacks such as phishing has pushed for the importance of cyber security. Several studies of phishing attacks have been carried out, but analysis of the phishing attack on the network and the identity of the attacker or phiser has not been revealed. Therefore, this research will analyze phishing web attacks on the e-commerce sector. Information relating to: URL, domain, IP Address, DNS, network protocol and the identity of the attacker or phiser will be disclosed based on the results of analysis of the data obtained during the acquisition. All stages of analysis will refer to the Network Forensic Process method. The success of this investigation and analysis process is shown by obtaining information about the sender's and recipient's email address and timestamp when a spam message is sent that directs to phishing activity. Besides that, information about fake domain (phishing host), IP Address, DNS and various protocols involved in transmitting data when phishing activities occur.

Keywords*— *Cybercrime, E-Commerce, Network Forensic, Phishing.

Intisari—*E-commerce* menyediakan fasilitas untuk menjangkau pelanggan di seluruh dunia tanpa batasan pasar geografis. Akibatnya, jumlah pelanggan yang bergantung pada internet untuk pembelian mengalami peningkatan yang signifikan. Potensi serangan *cybercrime* seperti *phishing*, telah mendorong pentingnya keamanan *cyber*. Beberapa penelitian terhadap serangan *phishing* sudah pernah dilakukan, tetapi analisa jejak serangan *phishing* pada jaringan dan identitas penyerang atau *phiser* belum dapat diungkapkan. Oleh karena itu, pada penelitian ini akan dilakukan analisa serangan web *phishing* pada sektor *e-commerce*. Informasi yang berhubungan dengan : URL, domain, *IP Address*, DNS, *network protocol* dan identitas penyerang atau *phiser* akan diungkapkan berdasarkan hasil analisis terhadap data yang diperoleh saat akuisisi. Seluruh tahapan analisis akan mengacu kepada metode *Network Forensic Process.* Keberhasilan proses investigasi dan analisis ini ditunjukan dengan diperoleh informasi mengenai alamat pengirim dan penerima email serta *timestamp* saat terjadi pengiriman pesan *spam* yang mengarahkan ke aktifitas *phishing*. Selain itu juga diperoleh informasi tentang *fake domain* (*host phishing*) *IP Address*, DNS serta berbagai protokol yang terlibat dalam trasmisi data saat terjadi aktifitas *phishing*.

Kata Kunci*—*Cybercrime, E-Commerce, Network Forensic Process, Phishing.

I. PENDAHULUAN

Peningkatan serangan *cybercrime* pada organisasi bisnis, infrastruktur pemerintah, dan individu telah menekankan pentingnya keamanan *cyber*, oleh karena itu analisis terhadap serangan *cyber* merupakan salah satu hal yang perlu dilakukan [1]. Bentuk *cybercrime* yang dilakukan oleh para *frauder* diantaranya *phishing*. *Phishing* merupakan kegiatan kriminal dengan menggunakan teknik rekayasa sosial [2]. Pengguna dirugikan dalam hal privasi, penyalahgunaan (eksploitasi) dari tindakan *hacking* bahkan kerugian finansial.

Hasil dari laporan [3] mengemukakan jumlah laporan *phishing* yang dikirimkan ke APWG selama kuartal pertama tahun 2018 sekitar 263.538 kasus serangan. Serangan tersebut mengalami peningkatan sekitar 46% dibanding kuartal keempat tahun 2017. Kasus serangan pada sektor *e-commerce* menjadi target utama yaitu sekitar 32, 4 % dari jumlah kasus yang terjadi.

Beberapa penelitian tentang serangan *phishing* pernah dilakukan sebelumnya, diantaranya : menggunakan metode s*ystematic litelatur review*[4], c*orrelation-based feature selection (CFS)*[5], *DBSCAN clustering method* [6]. Penelitian [4] mengemukakan faktor-faktor penyebab *phisihing*. Penelitian [5] berhasil menghilangkan *redundant* atribut pada *phishing*. Sedangkan penelitian [6] berhasil menemukan tingkat akurasi pendeteksi serangan *phishing*. Tetapi dari beberapa penelitian tersebut, analisa jejak serangan *phishing* pada jaringan dan identitas penyerang atau *phiser* belum dapat diungkapkan.

Network Fosensic Process merupakan suatu metode yang dapat digunakan untuk kegiatan investigasi dan analisa aktivitas *cyber crime*. Dimana bukti ditangkap dari jaringan dan diinterpretasikan berdasarkan pengamatan. Hal ini bertujuan untuk menemukan identitas penyerang dan merekonstruksi tindakan serangan melalui analisis bukti penyusupan. Metode *Network Forensic Process* lebih detail dan dapat digunakan untuk investigasi di jaringan dibandingkan dengan metode seperti DFRWS (*Digital Forensics Research Workshop*)[7]. Oleh karena itu, pada penelitian ini akan dilakukan analisa serangan *web phishing* pada sektor *e-commerce.* Pada tahap awal akuisisi data dilakukan guna memperoleh informasi tindakan *phishing* yang telah dilakukan. *Domain, IP Address, DNS, network protocol* dan identitas penyerang atau *phiser*, merupakan beberapa informasi yang akan diungkapkan berdasarkan hasil analisis yang dilakukan pada penelitian ini. Pada tahap akhir akan disajikan seluruh hasil analisis, sehingga dapat dibuktikan bahwa tindakan *phishing* yang terjadi benar-benar telah dilakukan. Seluruh tahapan analisis akan mengacu kepada metode *Network Forensic Process*.

II. LANDASAN TEORI

1) Phishing

Phishing adalah aktivitas *cyber crime* yang menggunakan rekayasa sosial dan tipuan teknis untuk mencuri data identitas dan kredensial akun keuangan. Skema rekayasa sosial dilakukan dengan menggunakan *e-mail* palsu yang mengaku berasal dari institusi bisnis yang sah dan dirancang untuk mengarahkan korban ke situs *web* palsu yang mengelabui, sehingga korban membocorkan data keuangan seperti : nama dan kata sandi. Skema *subterfomen* teknis menanam *crimeware* ke PC untuk mencuri kerahasiaan secara langsung, sering menggunakan sistem untuk mengelabui nama pengguna dan kata sandi akun *online* dan merusak infrastruktur navigasi lokal untuk menyesatkan konsumen ke situs *web* palsu (atau situs *web* asli melalui *proxy* yang dikendalikan *phiser* yang digunakan untuk memantau dan *intercept* pada konsumen)[3].

B. Teknik Phishing

Cyber crime yang dilakukan oleh seorang *phiser* menggunakan beberapa teknik antara lain:

1. *Email Spoofing*
   Teknik ini biasa digunakan *phiser* dengan cara mengirim *email* secara *broadcast* ke jutaan pengguna, seolah-olah berasal dari institusi resmi ang berisi seruan untuk melakukan sesuatu. Biasanya *e-mail* berisi pemintaan nomor kredit, *password* atau mengunggah *form* tertentu[8].
2. *Pengiriman Berbasis Web*
   Pengiriman berbasis web adalah salah satu teknik *phishing* yang paling canggih. Dikenal sebagai *"man-in-the-middle", phiser* terletak diantara situs *web* asli dan sistem *phishing*[8].
3. *Pesan Instan (chatting)*
   Olah pesan cepat adalah metode dimana pengguna menerima pesan berupa *link* yang diarahkan ke situs *web* palsu yang memiliki tampilan sama sehingga pengguna merasa mengakses situs *web* resmi yang sah padahal palsu[8].
4. *Trojan hosts*
   Trojan hosts, phiser mencoba login ke *account* pengguna untuk mengumpulkan kredensial melalui mesin lokal. Informasi yang diperoleh kemudian dikirim ke *phisher*[8].
5. *Manipulasi tautan (link)*
   Manipulasi *link* adalah teknik dimana *phisher* mengirimkan *link* ke sebuah *website*. Bila pengguna melakukan *click* pada *link* tersebut, maka akan diarahkan ke *website phisher* yang bukan *link website* sebenarnya[8].
6. *Malware Phishing*
   Penipuan yang melibatkan *malware* untuk dijalankan pada komputer pengguna. *Malware* ini biasanya melekat pada *e-mail* yang dikirimkan kepada pengguna oleh *phisher*. Setelah korban melakukan klik pada *link*, maka *malware* akan mulai berfungsi. *Malware* tersebut terkadang disertakan pada *file* yang dapat *download*[8].

C. E-commerce

Berikut pengertian *e-commerce* menurut para ahli:

1. Penggunaan jaringan komunikasi dan komputer untuk melaksanakan proses bisnis. Pandangan populer dari *e-commerce* adalah penggunaan *internet* dan komputer dengan *web browser* untuk membeli dan menjual produk[9].
2. Transaksi bisnis yang terjadi dalam jaringan elektronik, seperti *internet*. Setiap orang yang mengakses komputer dan terhubung ke *internet* serta memiliki cara untuk membayar barang-barang atau jasa yang dibeli, dapat berpartisipasi dalam *e-commerce*[10].
3. Pembelian, penjualan dan pemasaran barang serta jasa melalui sistem elektronik, seperti : radio, televisi dan jaringan komputer atau *internet*[11].

D. Network Forensic

Network forensics adalah cabang dari *digital forensics* yang berkaitan dengan *monitoring* dan analisis lalu lintas data di jaringan komputer untuk tujuan pengumpulan informasi, bukti hukum dan deteksi penyusupan terhadap jaringan komputer [12]. Proses forensik jaringan terdiri dari 3 tahap seperti ditampilkan pada gambar 1.

Gambar 1. Proses Forensik Jaringan[13]

Gambar 1 menampilkan tiga tahap proses forensik jaringan yang terdiri dari:

1. Akuisisi dan pengintaian (*reconnaissance*)
   Aktifitas yang dilakukan pada tahap ini yaitu pengumpulan informasi aktifitas *phishing* yang yang akan dianalisis. Pengumpulan data dapat dilakukan dengan dua cara yaitu : pengumpulan data dengan bekerja pada *system online (data volatile)* dan pengumpulan data dari *disk* yang terkait dengan

JUTEI Edisi Volume.2 No.2 Oktober 2018
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.22.111

aktifitas *phishing* secara *offline* dengan memanfaatkan berbagai *tools (data non-volatile).*

2. Analisa
   Kegiatan pada tahap ini yaitu mengamati secara detail data yang diperoleh dari proses *reconnaissance*, dengan cara menguraikan komponen-komponen pembentuknya atau penyusunnya untuk di kaji lebih lanjut. Analisa yang dilakukan meliputi : analisa aktifitas di jaringan komputer secara *online* maupun *offline*, analisa data rekaman jejak *phishing (volatile* atau *non-volatile)*, analisa *log-file*, korelasi data dari berbagai perangkat pada jaringan yang dilalui serangan dan pembuatan *timeline* dari informasi yang diperoleh.
3. *Recovery*
   Pada tahap ini dilakukan pemulihan kembali data yang telah hilang akibat adanya intrusi, khususnya informasi pada *disk* berupa *file* atau *directory*.

E. Network Protocol Analyzer

Network Protocol Analyzer adalah sebuah *tool* yang ditujukan untuk melakukan analisis paket data pada jaringan, contoh: *wireshark*. *Wireshark* dapat digunakan dalam pengawasan paket secara nyata (*real time*), menangkap data *(capture data)*, menampilkan data hasil *capture* dengan lengkap. *Wireshark* berbasis *open sources.* Aplikasi *wireshark* dapat digunakan di berbagai *platform* seperti : *linux, windows* dan *Mac*[14]. Beberapa contoh skenario yang dapat digunakan dengan *wireshark* diantaranya sebagai berikut:

1. Melakukan *troubleshoot* permasalahan jaringan.
2. Melakukan pengujian masalah keamanan jaringan.
3. Malakukan *debugging* implementasi protokol.
4. Belajar protokol jaringan.

Wireshark dapat digunakan untuk mendapatkan informasi sensitif pada jaringan seperti kata sandi, *cookie* dan sebagainya. Berikut sebagian fitur pada *wireshark*:

1. Tersedia untuk *platform* UNIX, Linux, Windows dan Mac.
2. Dapat melakukan *capture* paket data jaringan secara *real time*.
3. Dapat menampilkan informasi protokol secara lengkap.
4. Paket data dapat disimpan menjadi *file* selanjutnya dapat dibuka kembali jika diperlukan.
5. Penyaringan *(filter)* paket data jaringan berdasarkan kriteria tertentu.
6. Pencarian paket data dengan kriteria spesifik.
7. Pengaturan warna pada saat penampilan paket data sehingga mempermudah analisa paket data.
8. Menampilkan statistik paket data pada jaringan.
9. *Wireshark* memerlukan antarmuka fisik *(network interface card)* untuk menangkap paket data yang keluar masuk pada jaringan. *Wireshark* mendukung antar muka jaringan sebagai berikut: ATMoth, Bluetooth, Tautan (*link*) CiscoHDLC, DOCSIS, *Ethernet*, *FrameRelay*, IRDA, Tautan PPP, SS7, *TokenRing*, USB, LAN.
10. Selain antar muka fisik, *wireshark* juga mendukung antarmuka virtual, seperti: *loopback*, *pipes*, VLAN dan *WinCapRemote*.

III. METODOLOGI

A. Alur Proses Jaringan Forensik

Tahapan penyelesaian masalah pada penelitian ini menggunakan metode proses forensik jaringan yang terdiri dari tiga tahap, sebagai berikut :

1. *Akuisisi dan Pengintaian (Reconnaissance)*
   Pada penelitian ini, proses *reconnaissance* dilakukan secara *offline*. Pada tahap ini berhasil diperoleh data *non-volatile* berupa 6 *file* hasil *capture* serangan *phishing* yang telah terjadi (*.pcap) dan 1 *file* teks berisikan informasi nilai *hash* dari setiap *file capture* (*.txt).
2. *Analisa Data*
   Proses investigasi dan analisa dilakukan pada 6 *file* hasil*capture* (*.pcap) dan 1 file yang berisikan nilai *hash* (*.txt). yang berektensi (.pcap). Proses investigasi dan analisa file **.pcap* dilakukan menggunakan perangkat lunak *wireshark*, sehingga diperoleh. investigasi yang dilakukan berupa pencarian informasi : *URL* yang terlibat dalam aktifitas *phisihing*, *IP address*, identitas penyerang *(phiser)*, pencarian waktu dan tanggal serangan, *network protocol* (ICMP, TCP, UDP), DNS, FTP, SMTP, HTTP.
3. *Recovery / Presentasi dan Hasil Review*
   Bagian ini merupakan fase akhir dari *Network Forensic Process*. Pada tahap ini disajikan seluruh hasil investigasi dan dilakukan *review* terhadap seluruh proses analisa. Semua hasil analisa disajikan dengan bahasa yang dimengerti serta dijelaskan berbagai prosedur yang digunakan sampai pada kesimpulan dari proses penyidikan. Hasil analisa disajikan dalam bentuk tabel yang berisi kesimpulan hasil investigasi dari setiap *file capture*.

B. Hardware dan Software yang Digunakan

Perangkat keras yang digunakan pada penelitian ini 1 unit laptop acer type AO756 dengan spesifikasi seperti ditampilkan pada Tabel I.

Tabel I. Spesifikasi *Hardware* yang Digunakan

No	Item	Deskripsi
1.	Processor	Intel Celereon 877 1,4Ghz
2.	Memory	6 Gb
3.	Harddisk	500 Gb

Perangkat lunak yang digunakan pada penelitian ini ditampilkan pada Tabel II.

Tabel II. Spesifikasi *Software* yang Digunakan

No	Software	Version
1.	*Wireshark*	V.2.0.2
2.	HashCalc	V.2.02
3.	Google Chrome	V.70.0.3538.102

Selain dari itu terdapat beberapa web yang digunakan dalam menganalisis aktifitas *phishing* seperti ditampilkan pada tabel III.

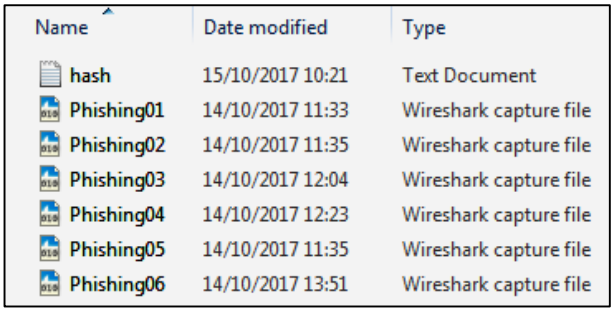
Tabel III. URL pemeriksaan link *phishing*

No	URL	Deskripsi
1.	www.centralops.net	Untuk memperoleh informasi dan investigasi domain
2.	www.pipl.com	Untuk pencarian identitas seseorang di internet
3.	www.tools.verifyemailaddress.io	Untuk memeriksa dan verifikasi data email.
4.	www.mywot.com	Untuk memeriksa tingkat ancaman atau kerentan aspek keamanan terhadap suatu domain

IV. HASIL DAN ANALISIS

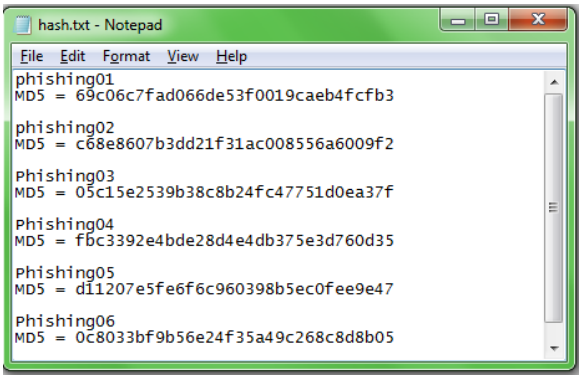
A. *Akuisisi data Pengintaian (Reconnaissance)*

Pada penelitian ini tahap akuisisi data dilakukan secara *offline*. Data *non-volatile* yang berhasil dikumpulkan pada tahap ini, diperoleh *group* tertutup di sosial media yang fokus membahas aktifitas *cyber crime*. Salah seorang anggota *group* tersebut berhasil melakukan *capture* terhadap aktifitas *phishing* secara *online*. Setelah melakukan diskusi pada *group* tersebut, maka diperoleh salinan 6 *file* hasil *capture* (*.pcap) serangan *web phishing* dan 1 file teks (*.txt) berisikan informasi nilai *hash* dari setiap file *capture* seperti ditampilkan pada gambar 2.



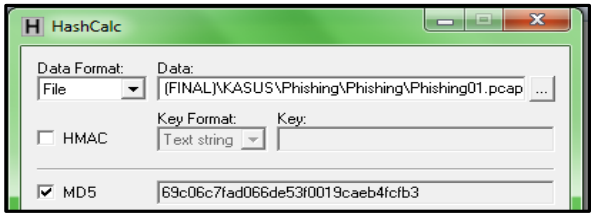
Gambar 2. Data Non-Volatile Serangan Phishing

Gambar 2 menampilkan 6 *file* hasil *capture* (*.pcap) yang dilakukan pada tanggal 14 oktober 2017 dengan *file type* berupa *wireshark capture file*. Selain dari itu berhasil diperoleh juga 1 *file* teks (*.txt) yang dibuat pada tanggal 15 Oktober 2017.



Gambar 3. Nilai *Hash* File Capture *Phishing*

Gambar 3 menampilkan informasi nilai *hash* dari setiap *file capture* (*.pcap) yang tersimpan dalam *file* hash.txt. Nilai *hash* yang dibuat menggunakan algoritma MD5. Tahapan berikutnya yaitu memeriksa nilai *hash* dari *file* data *non-volatile* (*.pcap). Pemeriksaan ini dilakukan untuk memastikan bahwa informasi nilai *hash* yang terdapat pada *file hash.txt* sama dengan nilai *hash* sebenarnya yang dimiliki setiap *file* *.pcap. Contoh hasil akuisisi nilai *hash* dari *file capture* Phishing01.pcap dengan menggunakan *tool HashCalc* ditampilkan pada gambar 4.



Gambar 4.Nilai *Hash* File Phishing01.pcap

Gambar 4 menampilkan informasi nilai *hash* MD5 **69c06c7fad066de53f0019caeb4fcfb3** yang dimiliki *file capture* phishing01.pcap menggunakan *tool HashCalc*. Informasi nilai *hash* MD5 yang ditampilkan untuk *file* phishing01.pcap dengan menggunakan HashCalc sama dengan informasi nilai *hash* MD5 yang ditampilkan pada *file* hash.txt. Ini artinya isi file Phishing01.pcap masih asli belum di *override* atau isi *file* tersebut belum dimodifikasi. Proses akusisi selanjutnya dilakukan pada setiap *file capture* (*.pcap), kemudian setiap nilai *hash* yang diperoleh dicatat dan ditampilkan seperti pada Tabel IV.

Tabel IV. Hasil Akuisisi Data Menggunakan HashCalc

File	Nilai Hash
Phishing01.pcap	69c06c7fad066de53f0019caeb4fcfb3
Phishing02.pcap	c68e8607b3dd21f31ac008556a6009f2
Phishing03.pcap	05c15e2539b38c8b24fc47751d0ea37f
Phishing04.pcap	fbc3392e4bde28d4e4db375e3d760d35
Phishing05.pcap	d11207e5fe6f6c960398b5ec0fee9e47
Phishing06.pcap	0c8033bf9b56e24f35a49c268c8d8b05

Tabel IV menampilkan informasi nilai *hash* hasil akuisisi dari setiap *file capture* (*.pcap) dengan menggunakan *tool HashCalc*. Setelah dilakukan perbandingan, nilai *hash* yang terdapat pada *file hash.txt* diketahui sama dengan nilai *hash* yang ditampikan pada Tabel IV. Ini artinya setiap *file capture* (*.pcap) merupakan *file* asli belum di *override* atau isi *file* tersebut belum dimodifikasi.

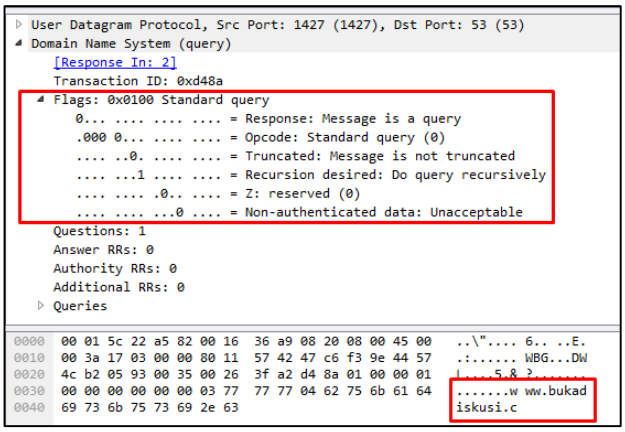
B. *Analisis*

1. *File Capture Phishing01.pcap*

File phishing01.pcap menyimpan 57 informasi paket data. Paket data nomor 1 merupakan sebuah *query request* kepada *DNS Server*. Ini berarti *file* phishing01.pcap merupakan *file* hasil *capture* ketika terjadi komunikasi menggunakan protokol DNS yang digunakan oleh *phiser* untuk melakukan serangan *phishing*. Informasi detail setiap *query* dapat diperoleh dengan cara klik *Domain Name*

JUTEI Edisi Volume.2 No.2 Oktober 2018
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.22.111

System (query), hasilnya seperti ditampilkan pada gambar 5.

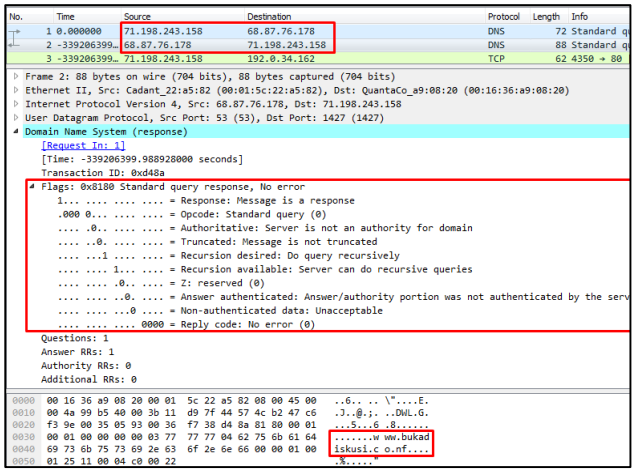


Gambar.5. Data lengkap protokol DNS dari data paket nomor 1

Gambar 5 menampilkan format *header* pada paket data yang berisi informasi protokol DNS. Diketahui bahwa aktifitas tersebut melakukan *query* terhadap domain www.bukadiskusi.co.nf. Analisa terdapat *query* tersebut sebagai berikut:

1. ***Flags*** bernilai 0x0100, memiliki arti:
   a. ***QR*** bernilai 0 berupa *query.*
   b. ***X*** menunukan nilai **Opcode 000** yaitu berupa *query.*
   c. TC bernilai 0 artinya *Not Truncated.*
   d. ***RD*** bernilai 1 artinya *Rercursion not desired.*
   e. ***AA*** bernilai 0 artinya *Not Authoritative.*
2. ***Question RRs*** bernilai 1.
3. ***Authority RRs*** bernilai 0.
4. ***Addtional RRs*** bernilai 0.

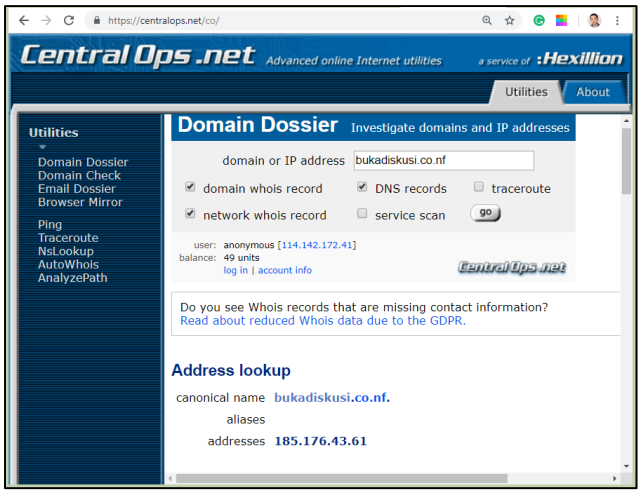
Selanjutnya untuk melihat respon dari paket data nomor 1, klik paket data nomor 2 maka akan diperoleh hasil format *header DNS* seperti ditampilkan pada gambar 6.



Gambar 6. Data respon dari DNS query paket data nomor 1

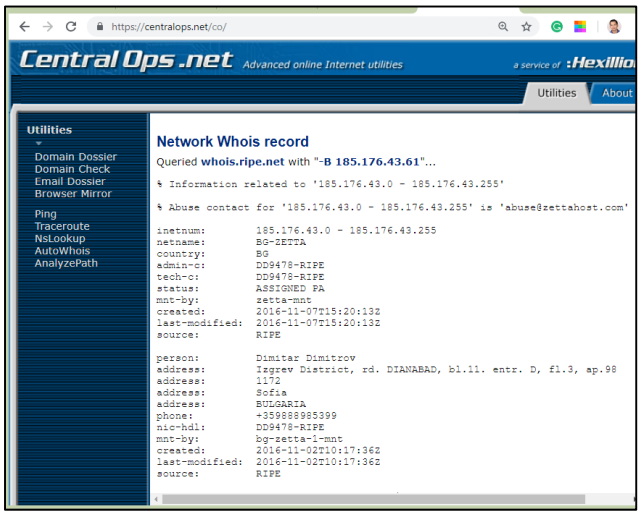
Gambar 6 menampilkan informasi detail hasil respon paket data nomor 1. Diketahui bahwa respon DNS *query* www.bukadiskusi.co.nf dengan ***IP address source*** **71.198.243.158** dan ***IP address destination*** **68.87.76.178**. Dengan hasil analisa protokol DNS sudah diketahui DNS yang digunakan oleh *phiser* dalam melakukan serangan sehingga disimpulkan untuk file phishing01.pcap merupakan file *capture* **Protokol DNS**.

Tahap selanjutnya setelah diketahui DNS *phishing* yaitu mencari informasi lebih lanjut mengenai DNS tersebut menggunakan *dnslookup*. Informasi dari *dnslookup* diperoleh dengan menggunakan fasilitas yang disediakan website https://centralops.net. Setelah mengakses URL tersebut dan memasukan domain bukadiskusi.co.nf pada kolom pencarian domain, maka diperoleh informasi seperti ditampilkan pada gambar 7.



Gambar 7. Informasi IP Address domain bukadisuksi.co.nf hasil DNSLookup

Gambar 7 menampilkan informasi, domain bukadiskusi.co.nf menggunakan *server* dengan *IP Address* 185.176.43.61. Bila tampilan informasi pada web seperti ditampilkan pada gambar 7 digeser ke bawah, maka akan diperoleh informasi lainnya, mengenai domain tersebut, seperti ditampilkan pada gambar 8.



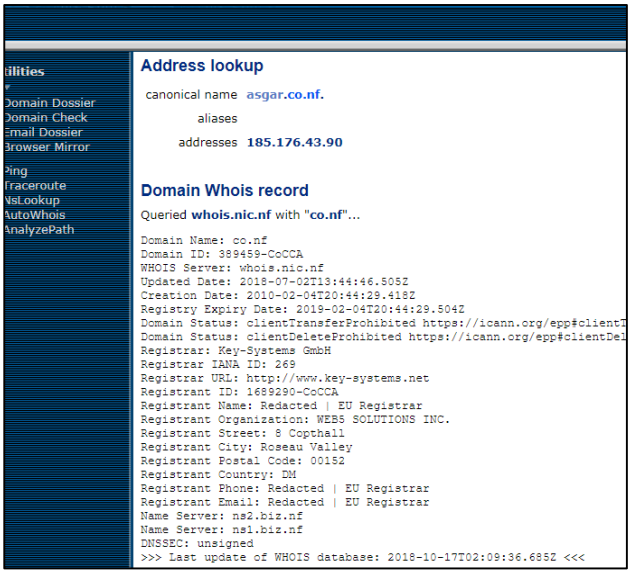
Gambar 8. Informasi Network Whois record domain bukadisuksi.co.nf hasil DNSLookup

Gambar 8 menampilkan informasi *Network Whois record* yang berhubungan dengan domain

bukadiskusi.co.nf. Dari data tersebut, diperoleh beberapa informasi penting diantranya:

a. Nama pendaftar domain : Dimitar Dimitrov
b. Alamat : Izgrev District, rd. DIANABAD, bl.11. entr. D, fl.3, ap.98 1172 Sofia
c. Negara : Bulgaria
d. Telp. : +359888985399
e. Tgl. Dibuat : 02-11-2016

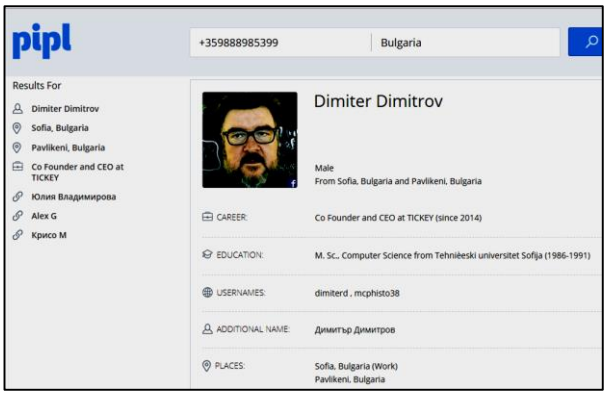
Pemerikasaan lebih lanjut mengenai informasi URL *phishing* dilakukan terhadap domain .co.nf dengan sengaja dibuat satu domain baru menggunakan co.nf. yaitu asgar.co.nf. Hasil dnslookup domain asgar.co.nf melalui https://centralops.net ditampilkan pada gambar 9.



Gambar 9. DNSLookup URL www.asgar.co.nf

Gambar 9 menampilkan informasi web www.asgar.co.nf yang sengaja dibuat dengan domain .co.nf. Setelah dibandingkan informasi *nslookup* dengan web bukadiskusi.co.nf ternyata diperoleh hasil data *source* yang yang sama. Hasil pemeriksaan tersebut sama dengan informasi dari web *phishing*, artinya data *source* yang dihasilkan proses *dnslookup* bukan merupakan data pemilik web atau URL tetapi data pemilik *hosting*. Jadi Dimitar Dimitrov bukanlah nama pendaftar domain bukadiskusi.co.nf tetapi pemilik *hosting* untuk domain co.nf.

Pemeriksaan lebih detail mengenai data *source* hasil *dnslookup* dilakukan pada identitas data *phone*. Investigasi dilakukan dengan bantuan fasilitas yang tersedia di web www.pipl.com. Informasi hasil pencarian berdasarkan data *phone* dan lokasi ditampilkan pada gambar 10.

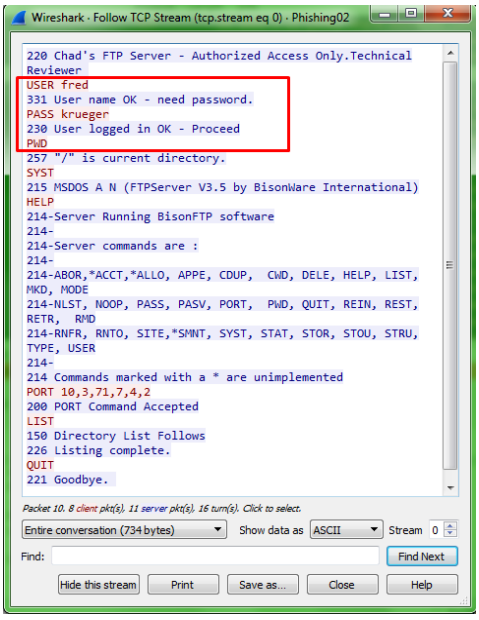


Gambar 10. Informasi Data Person Berdasarakan Data Phone +359888985399

Gambar 10 menampilkan hasil pencarian dengan parameter data *phone* dan lokasi. Informasi yang ditunjukan sama dengan hasil data *source dnslookup*, artinya data identitas yang ditampilkan tersebut merupakan data dari pemilik domain .co.nf.

2. File Capture Phishing02.pcap

File Phishing02.pcap menyimpan informasi dari 42 paket data. Aktivitas di jaringan yang tercatat dalam paket data tersebut dianalisa. Analisa difokuskan pada paket data nomor 3-5, yang menampilkan informasi dari IP Address 10.3.71.7 yang melakukan *request* ke *File Transfer Protokol (FTP) Server* melalui protokol TCP/IP. Paket data nomor 6 menampilkan informasi respon dari *FTP server* ke *client*. Informasi detail isi paket data nomor 6 dapat ditampilkan dengan memilih menu ***follow tcp stream,*** sehingga diperoleh data seperti ditunjukan pada gambar 11.



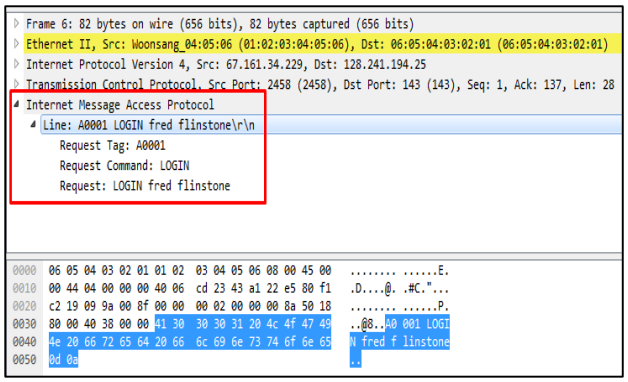
Gambar 11. Isi Paket data Nomor 6 Protokol FTP

Gambar 11 merupakan *history* dari komunikasi layanan protokol FTP. *File capture* Phishing02.pcap. Diketahui ***Username* = Fred** dan ***Password* = krueger** digunakan oleh *phiser* untuk mengakses FTP *Server*.

JUTEI Edisi Volume.2 No.2 Oktober 2018
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.22.111

3. File Capture Phishing03.pcap

File phishing03.pcap menyimpan informasi dari 22 paket data. Paket data nomor 1-3 menyimpan informasi komunikasi jaringan menggunakan protokol TCP dengan ***IP Address Source*** 67.161.34.229 dan ***IP Address Desination*** 128.241.194.25 untuk melakukan koneksi dari klien ke server menggunakan protokol *Internet Message Access Protocol* (IMAP). IMAP merupakan salah satu standar protokol internet yang digunakan oleh klien email untuk mengambil pesan email dari server email melalui koneksi TCP/IP. Paket data nomor 4, menampilkan informasi koneksi antara klien dan server yang terjalin sehingga komunikasi dapat dilakukan, seperti ditampilkan pada gambar 12.

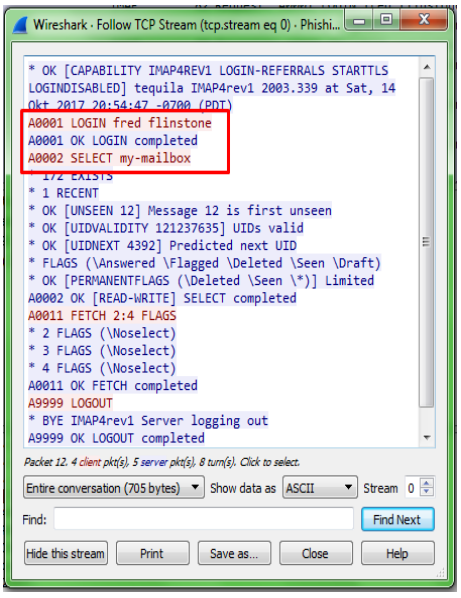


Gambar 12. Koneksi dari Klien ke Server menggunakan protokol IMAP

Gambar 12 menampilkan informasi koneksi yang dilakukan klien ketika login ke email *server*. Informasi *request* yang dilakukan sebagai berikut:

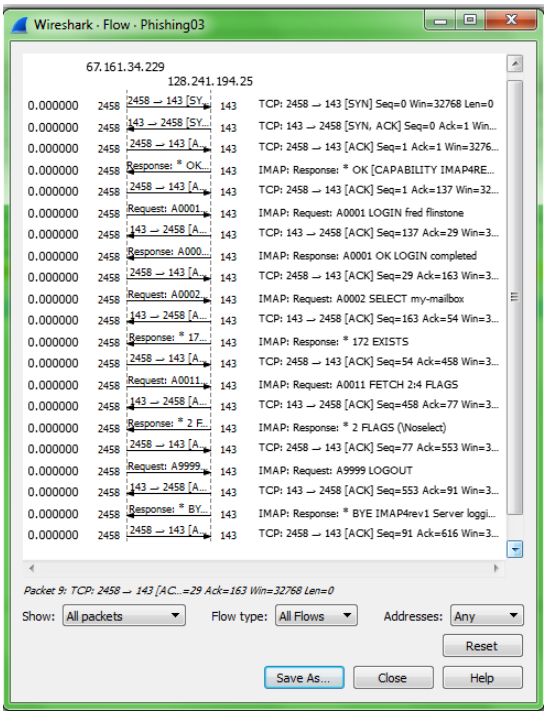
- *Request Tag* : A0001
- *Request Command* : LOGIN
- *Request* : LOGIN fred flinstone

Informasi detail dari aktifitas komunikasi yang melibatkan protokol IMAP dapat diketahui dengan cara memilih menu ***follow tcp stream*.** Informasi yang diperoleh ditampilkan pada gambar 13.



Gambar 13. Isi Paket data Nomor 4 protokol IMAP

Gambar 13 menampilkan informasi waktu, nama serta password yang digunakan untuk mengakses email server menggunakan protokol IMAP. Diketahui bahwa login ke email server dilakukan pada **Sat, 14 Okt 2017 20:54:47,** dengan ***User name*** = **Fred** dan ***password*** = **flinstone.** Lebih jelas mengenai interaksi jaringan pada protokol SMTP dapat dilakukan dengan cara melihat data *flow graph* seperti pada gambar 14.

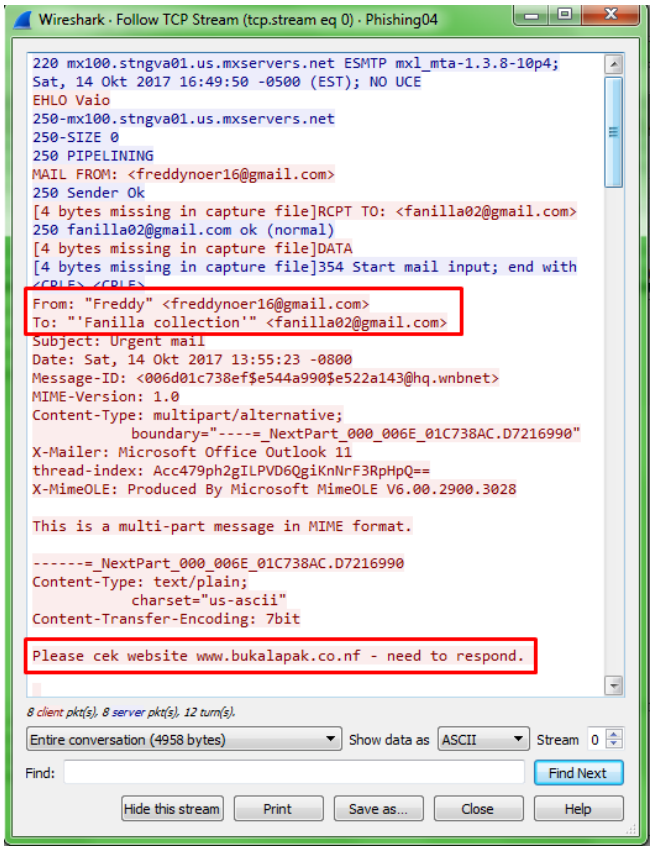


Gambar 14. Flow Graph Paket Data SMTP

Gambar 14 menampilkan *flow graph* ketika terjadi transmisi data yang melibatkan protokol TCP dan IMAP. Dari data tersebut diketahui transmisi data dilakukan antara klien IP Address 128.241.194.25 dengan email server IP Address 67.161.34.229. Hasil analisa bahwa, isi dari *file capture* Phsihing03.pcap menyimpan informasi komunikasi saat terjadi komunikasi antara klien dan server email yang melibatkan protokol IMAP dan TCP yang dilakukan oleh *phiser.*

4. File Capture Phishing04.pcap

File phishing04.pcap menyimpan informasi dari 31 paket data. Paket data tersebut terdiri dari rekaman aktifitas komunikasi yang melibatkan protokol TCP dan SMTP dengan *IP address Source* 67.161.34.229 dan *IP Address Destination* 128.241.194.25. Paket data nomor 1-3 berisi rekaman komunikasi menggunakan protokol TCP ketika terjadi koneksi dari klien ke server SMTP. Setelah koneksi antar klien dan server terhubung, server SMTP memberikan respon kepada klien. Informasi yang tersimpan dalam paket nomor 4 ditampilkan pada gambar 15.

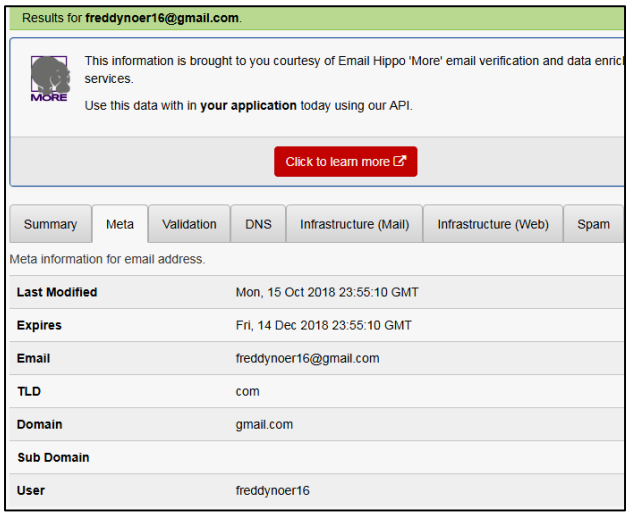


Gambar 15. Isi Paket data Nomor 4 Protokol SMTP

Gambar 15 menampilkan informasi rekaman aktifitas komunikasi antara klien dan *SMTP server*. Komunkasi diawali dengan kode 220 yang berarti *SMPT Server* siap menerima *request* dari klien (*server ready)* yang terjadi pada Sat, 14 Okt 2017 16:49:50. Kemudian klien mengirim perintah *EHLO* dengan parameter *vaio*.

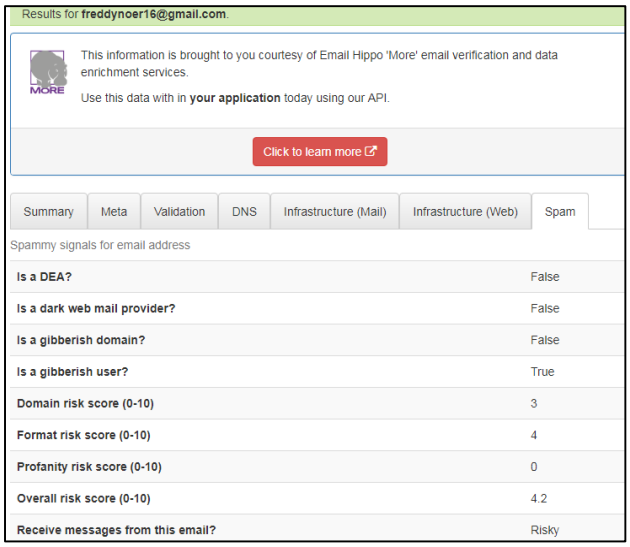
Perintah EHLO digunakan untuk mengidentifikasi pengirim SMTP kepada *SMTP Server*. *Argument field* berisi *host name* pengirim SMTP. Penerima SMTP mengidentifikasi dirinya sendiri ketika membalas *connection greeting* dan merespon perintah ini. Perintah akan dibalas dengan OK untuk mengkonfirmasi keduanya. Hal ini ditunjukan pada baris ke-5 dengan kode 250 diikuti dengan *webserver*.

Informasi yang perlu diperhatikan dari tampilan gambar 15 yaitu alamat pengirim dan penerima email. Diketahui terdapat sebuah pesan *email* berasal dari **freddynoer16@gmail.com** kepada **fanilla02@gmail.com** dan *subject* ***Urgent Mail***. Isi dari email yang dikirimkan yaitu ***"Please check website www.bukalapak.co.nf - need to respon"***. Isi pesan tersebut berarti mengarahkan penerima email untuk mengakses web www.bukalapak.co.nf. Merujuk dari hasil tersebut bisa diketahui isi file *capture* dari phishing04.pcap merupakan file *capture* layanan **Protokol SMTP.** Pemeriksaan lebih lanjut mengenai informasi identitas alamat email dilakukan dengan memanfaatkan layanan dari web https://tools.verifyemailaddress.io seperti ditampilkan pada gambar 16.



Gambar 16. Meta Data Email Penyerang Phishing

Gambar 16 menampilkan informasi detail dari suatu akun email. Informasi tersebut terdiri dari: **user = freddynoer16**, **domain = gmail.com, last modified = Mon, 15 Oct 2018**. Dari data tersebut diketahui bahwa akun email **freddynoer16@gmail.com** terkahir kali diakses sesuai pada tanggal yang tercantum di item *last modified*. Tahap lebih lanjut untuk mengetahui informasi tingkat kerentanan dari suatu akun email bisa dilakukan dengan memilih menu *spam*, hasilnya seperti ditunjukan pada gambar 17.



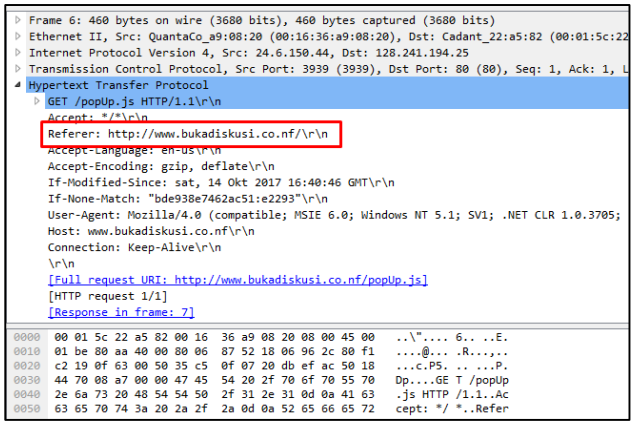
Gambar 17. Tingkatan Resiko Penggunaan Spam melalui Email

Gambar 17 menampilkan penilaian tingkat pengiriman *spam* yang dilakukan oleh suatu akun email. Akun email **freddynoer16@gmail.com**, termasuk kategori "*gibberish user*", *domain risk score* = 3, *format risk score* = 4 dan hasil penilian dengan parameter *Receive messages from this email? = Risky*. Jadi artinya apabila menerima pesan dari **freddynoer16@gmail.com** harus berhati-hati karena email yang dikirimkan berpotensi *spam*.

JUTEI Edisi Volume.2 No.2 Oktober 2018
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.22.111

5. *File Capture Phishing05.pcap*

File phishing05.pcap menyimpan informasi dari 361 paket data. Informasi yang tersimpan berisi rekaman komunikasi yang melibatkan protokol DNS, HTTP dan TCP. Pada paket data nomor 1 dan 2, menjelaskan koneksi *request* yang dilakukan dari komputer dengan IP Address 24.6.150.44 kepada DNS Server untuk mendapatkan alamat *IP Address* dari domain www.bukadiskusi.co.nf. Setelah diketahui bahwa domain www.bukadiskusi.co.nf memiliki IP Addres 128.241.194.25, koneksi dilakukan melalui protokol TCP yaitu terdapat pada paket data nomor 3-5. Pada paket data nomor 6, ditampilkan komunikasi selanjutnya yang dilakukan *IP Address* 24.6.150.44 kepada *web server* menggunakan protokol HTTP seperti ditunjukan pada gambar 18.



Gambar 18. Paket Header HTTP

Gambar 18 menunjukan HTTP *request* ke file */popup.js* dengan metode GET. Informasi penting terkait *entitiy header* pada paket data tersebut ditampilkan pada Tabel V.

Tabel V. *Entity Header* HTTP

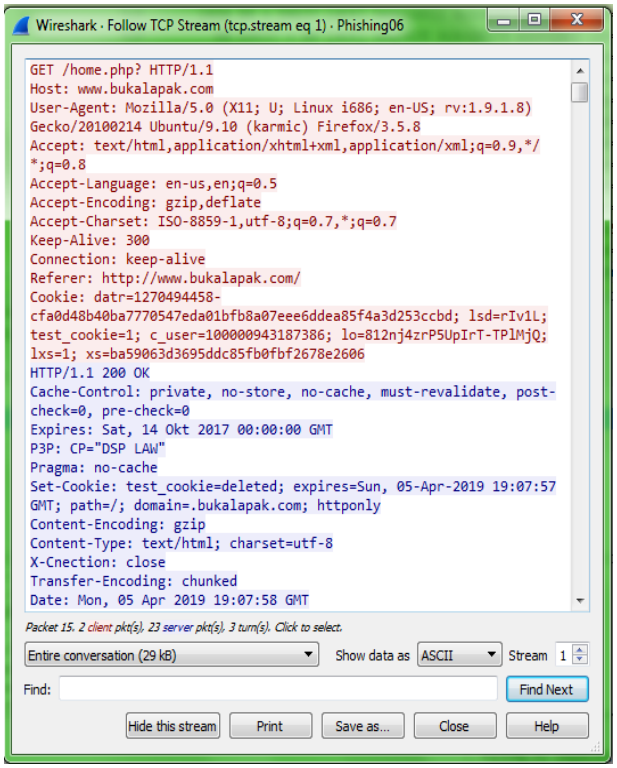
Entity Header	Value
Accept	*/*\r\n
Referer	http://www.bukadiskusi.co.nf/\r\n
Accept-Language	en-us\r\n
Accept-Encoding	Gzip, deflate\r\n
If-Modified-Since	Sat, 14 Okt 2017 16:40:46
User-Agent	Mozila/4.0

Tabel V menampilkan *entity header* dari isi paket data *request* HTTP yang menunjukan sebuah *website phishing* dengan *domain* www.bukadiskusi.co.nf. Setiap komunikasi HTTP selalu teridiri atas *request* dan *response*. Hasil analisis isi dari file *capture* Phishing05.pcap, bahwa telah terjadi koneksi antara klien dengan IP Address 24.6.150.44 kepada *server* www.bukadiskusi.co.nf dengan IP Addres 128.241.194.25 melalui protokol HTTP.

6. *File Capture Phishing06.pcap*

File phishing06.pcap menyimpan informasi dari 71 paket data. Informasi yang tersimpan dalam paket data ini berkaitan dengan protokol TCP, TSLv1 dan HTTP. Pada paket data nomor 4, ditampilkan protokol TLSv1 dengan melakukan *TCP stream* ke sebuah *link* menuju *form* login dari *website* www.bukalapak.com dengan *IP Address Source* 172.16.0.122 dan *IP Address Destination 69.63.180.173*.

Paket data nomor 59 dengan protokol HTTP terdapat perintah *GET /home.php* menunjukan adanya suatu *request* yang ditujukan ke suatu web. Informasi detail dapat diketahui dengan memilih menu *follow tcp stream*, sehingga diperoleh informasi seperti ditampilkan pada gambar 19.



Gambar 19. Isi Paket data Nomor 59

Gambar 19 menampilkan infomasi *request* dengan metode GET dari suatu klien ke domain www.bukalapak.com. *Entity Header* pada paket data tersebut ditampilkan pada Tabel VI.

Tabel VI. *Entity File Header Home.php*

Entity Header	Value
Request Protokol	GET /home.php? HTTP/1.1
Host	www.bukalapak.com
User-Agent	Mozilla/5.0 Linux i686 Ubuntu/9.10 (karmic) firefox/3.5.8
Accept-Language	en-us
Accept-Encoding	gzip,deflate
Accept-Charset	ISO-8859
Referer	http://www.bukalapak.com/
Expires	Sat, 14 Okt 2017 00:00:00 GMT

C. *Presentasi dan Review (Recovery)*

Proses investigasi dan analisis dari setiap *file capture* (*.pcap) telah selesai dilakukan. Terdapat berbagai

informasi serta protokol jaringan yang terlibat berdasarkan hasil analisis yang telah dilakukan seperti ditampilkan pada Tabel VII.

Tabel VII. Review Hasil Investigasi dan Analisis

File	Hasil
Phishing01.pcap	• Protokol DNS (*Domain Name System*) • Host Phishing www.bukadiskusi.co.nf • IP address Source = 71.198.243.158 • IP Destination = 68.87.76.178 • User-Agent = Mozilla/4.0 • Server Apache/1.3.27 (Unix) (Red-hat/Linux) • Person Domain = Dimitar Dimitrov • Address = BULGARIA • Create = 2016-11-02T10:17:36Z
Phishing02.pcap	• Protokol FTP (File Transfer Protocol) • IP address Source = 10.30.3.1 • IP Destination = 10.3.71.7 • Username FTP = Fred • Password FTP = krueger
Phishing03.pcap	• Protokol IMAP (Internet Message Access Protocol) • IP address Source = 128.241.194.25 • IP Destination = 67.161.34.229 • File Login mailbox username = Fred Flinstone • Date : Sat, 14 Okt 2017 20:54:47
Phishing04.pcap	• Protokol SMTP • Mail Server: mx100.stngva.us.mxservers.net • IP address Source = 128.241.194.25 • IP Destination = 67.161.34.229 • X-mailer = Microsoft Office Outlook 11 • Mail From = “Freddy” Freddynoer16@gmail.com • Mail To = “Fanilla Collection” Fanilla02@gmail.com • Date : Sat, 14 Okt 2017 13:55:23
Phishing05.pcap	• Protokol HTTP (Hypertext Transfer Protocol) • Referer : http://www.bukadiskusi.co.nf/ • Host : www.bukadiskusi.co.nf • User-Agent: Mozilla/4.0 • Accept-Language: en-us • Accept-Encoding: gzip, deflate • Date : Sat, 14 Okt 2017 16:40:46 GMT
Phishing06.pcap	• Protokol HTTP, File Login • IP address Source = 172.16.0.122 • IP Destination = 69.63.180.173 • Host: www.bukalapak.com • User-Agent: Mozilla/5.0 (X11, Linux i686) Firefox/3.5.8 Ubuntu 9.10 (Karmic) • Accept-Language: en-us • Accept-Endcoding: gzip, deflate • Accept-Charset: ISO-8859 • Referer : http://www.bukalapak.com/

Tabel VII menampilkan beberapa protokol yang terlibat dalam komunikasi di jaringan diantaranya: DNS, FTP, IMAP, SMTP dan HTTP. Dari enam *file* hasil *capture* (*.pcap) tersebut diketahui :

1. Pada tanggal 02-11-2016 telah dibuat suatu host *phishing* www.bukadiskusi.co.nf. Berdasarkan hasil investigasi, domain co.nf terdaftar atas nama: Dimitar Dimitrov yang berlokasi di Bulgaria.
2. Diketahui sebuah akun yang digunakan untuk mengakses FTP server. *User name* dari akun tersebut adalah **Fred** dengan *password* **kruger.**
3. Telah terjadi pengiriman pesan melalui email. Pesan dikirim menggunakan alamat pengirim = **freddynoer16@gmail.com** yang ditujukan kepada penerima yang beralamat di fanilla02@gmail.com pada tanggal 14 Oktober 2017 dengan *subject : **Urgent Mail***. Pesan yang dikirimkan yaitu ***“Please check website www.bukalapak.co.nf - need to respon”***. Isi pesan tersebut berarti mengarahkan penerima email untuk mengakses web www.bukalapak.co.nf**.**
4. Telah terjadi aktifitas *phishing* pada domain www.bukalapak.com, dimana pengguna diarahkan kepada domain www.bukadiskusi.co.nf yang terjadi pada 14 Okt 2017 16:40:46 GMT.

V. KESIMPULAN

1. Hasil investigasi dan analisis dari akuisisi data, diketahui telah terjadi pengiriman pesan melalui email dari freddynoer16@gmail.com kepada fanilla02@gmail.com pada tanggal 14 Oktober 2017. Isi pesan mengarahkan penerima email untuk mengakses web www.bukalapak.co.nf yang merupakan web palsu dari web *e-commerce* www.bukalapak.com. Ketika diakses pengguna akan diarahkan ke web *phishing* yang didaftarkan pada domain co.nf yang berlokasi di bulgaria. Alamat host yang dibuat untuk phishing www.bukadiskusi.co.nf.
2. Tantangan pada penelitian selanjutnya, perlu dilakukan penelusuran atau pencarian informasi lebih detail ketika diperoleh suatu informasi *fake domain*, selain dari itu juga perlu digali lebih jauh tentang informasi identitas personal yang terlibat dalam aktifitas *phishing*.

DAFTAR PUSTAKA

[1] E.-C. University, “4 Reasons Why You Should Consider Cybersecurity as a Profession,” 5 December 2017. [Online]. Available: https://www.eccu.edu/4-reasons-why-you-should-consider-cybersecurity-as-a-profession/. [Diakses 13 September 2018].

[2] Singh, “Online Frauds in Banks with Phishing,” *Journal of Internet Banking and Commerce*, p. 4, 2007.

[3] APWG, “Phishing Activity Trends Report,” Wasington D.C, 2018.

[4] I. Radiansyah, Candiwan dan Y. Priyadi, “Analisis Ancaman Phishing dalam Layanan Online Banking,” *UMM Scientific Journals*, pp. 1-14, 2016.

JUTEI Edisi Volume.2 No.2 Oktober 2018
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.22.111

[5] B. M. Susanto, "Identifikasi Website Phishing dengan Seleksi Atribut Berbasis Korelasi," *SENTIKA*, 2016.

[6] G. Liu, B. Qiu dan L. Wenyin, "Automatic Detection of Phishing Target from Phishing Webpage," *Internation Conference on Pattern Recognation*, 2010.

[7] Singh, "Network Forensics," *Indian Computer Response Team (CERT-In) Department of Information Technology*, 2009.

[8] Pretty, Emmanuel dan Joshi, "Forensic Analysis of Email Date and Time Spoofing," *Proceedings of the 2012 Third International Conference on Computer and Communication*, 2012.

[9] P. McLeod, Sistem Informasi Manajemen, Jakarta: Salemba, 2008.

[10] S. C. Thomson, Discovering Computer, Jakarta : Salemba, 2008.

[11] W. Jony, Internet Marketing for Beginner, Jakarta: PT Alex Media Komputindo, 2010.

[12] A. Kurniawan, Network Forensic Menggunakan Wireshark, Yogyakarta: Andi, 2012.

[13] Chriscelda, "Network Forensik," 16 November 2014. [Online]. Available: https://fingersings.wordpress.com/2014/11/16/network-forensik/. [Diakses Desember 2017].

[14] A. Singh, Instant Wireshark Starter, Birmingham - Mumbai: Packt Publishing, 2013.

[15] B. Ruchandani, M. Kumar, A. Kumar, K. Kumari, A. K. Sinha dan P.Pawar, "Ekperimentation in network forensics analysis," dalam *Proceedings of the Term Paper Series under CDAC-CNIE Bangalore*, India, 2006.

[16] F. Sulianta, Komputer Forensik, Jakarta: Elex Media Komputindo, 2008.

[17] M. N. Al-Azhar, Digital Forensic: Panduan Praktis Investigasi Komputer, Jakarta: Salemba Infotek, 2012.