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

ANALISIS *WEB PHISHING* MENGGUNAKAN METODE *NETWORK FORENSIC* DAN *BLOCK ACCESS* SITUS DENGAN ROUTER MIKROTIK

Sutarti[1], Siswanto[2], Ariansyah Bachtiar[3]
Program Studi Sistem Komputer, Fakultas Teknologi Informasi Universitas Serang Raya
E-mail: sutarti86@gmail.com[1], fitraakbar06@gmail.com[2], ariansyahb4@gmail.com[3]

Abstrak - *Web phishing* adalah situs web yang dirancang untuk melakukan bentuk penipuan dengan cara percobaan untuk mendapatkan informasi sensitif. Dimana proses *phishing* ini bermaksud untuk menangkap informasi yang sangat sensitif seperti *username, password* dan detil kartu kredit dalam bentuk menyamar sebagai sebuah entitas yang dapat dipercaya/ *legitimate organization* dan biasanya berkomunikasi secara elektronik. Oleh karena itu penulis melakukan analisis menggunakan metode *network forensic*. Penelitian forensik jaringan dilakukan menggunakan metode model proses forensik *(The Forensic Process Model*), sebuah model proses investigasi forensik digital, yang terdiri dari tahap pengkoleksian, pemeriksaan, analisis dan pelaporan. Penelitian dilakukan selama lima bulan dengan mengambil data berupa *file capture* dari *Network Protocol Analyzer* (*Wireshark*). *Wireshark* mengizinkan pengguna mengamati data dari jaringan yang tengah beroperasi atau dari data yang ada di *disk*, dan segera melihat/mensortir data yang tertangkap, mulai dari informasi singkat dan rincian untuk segala hal tentang paket termasuk juga *full header* & jumlah data, bisa didapat. Berdasarkan hasil penelitian yang telah dilakukan, terdapat *IP address* yang melakukan tindakan *phishing*. Untuk mencegahnya pencurian data maka digunakan *router* mikrotik guna memblokir *web phishing* dan berperan sebagai *network* (jaringan), pengendali, atau pengatur lalu lintas antar jaringan. Dalam penelitian ini penulis berhasil mendapatkan identitas pembuat *web phishing* dan berhasil melakukan *blocking* terhadap *web* tersebut.

Kata Kunci: Mikrotik, *Network Forensic*, *Phishing*, Wireshark

I. PENDAHULUAN

Landasan forensik digital ialah praktik pengumpulan, analisis, dan pelaporan data digital. Investigasi forensik digital memiliki penerapan yang sangat beragam. Bidang ilmu forensik atau forensik adalah istilah yang diberikan untuk penyelidikan kejahatan menggunakan sarana ilmiah atau digunakan untuk menggambarkan deteksi kejahatan secara umum. *Computer Forensics Secrets & Solutions* secara umum sub digital forensik terbagi menjadi lima yaitu *live forensic*, *network forensic*, *computer forensic*, *mobile forensic, dan database forensic*. Dengan perkembangan teknologi berbasis digital, kejahatan telah menjadi ancaman bagi masyarakat karena dapat berdampak pada kerusakan yang cukup besar. Hal tersebut dapat terjadi desebabkan oleh tingkat pertumbuhan ilmu teknologi yang begitu signifikan sehingga untuk menggungkap kejahatan yang ditimbulkan sangatlah sulit (Phillip Cowen, dan Davis, 2009).

Pada saat ini perkembangan Ilmu Pengetahuan dan Teknologi (IPTEK) yang cukup pesat sudah menjadi realita sehari-hari bahkan merupakan tuntutan masyarakat yang tidak dapat ditawar lagi. Tujuan utama perkembangan iptek adalah perubahan kehidupan masa depan manusia yang lebih baik, mudah, murah, cepat dan aman. Perkembangan iptek terutama teknologi informasi (*Information Technology*) seperti internet berkembang begitu pesat. Hampir semua bidang kehidupan memanfaatkan teknologi informasi dalam menjalankan aktifitasnya. Mulai dari bidang ekonomi, pendidikan, kesehatan, pemerintahan, perbankan, agama dan juga sistem pertahanan dan keamanan suatu Negara.

Dengan kemajuan teknologi informasi yang serba digital membawa orang ke dunia bisnis yang *revolusioner* (*digital revolution era*) karena dirasakan lebih mudah, murah, praktis dan dinamis berkomunikasi dan memperoleh informasi. Akan tetapi di balik manfaat-manfaat itu semua, terkadang ada beberapa pihak tertentu yang menyalahgunakan penggunaan teknologi informasi dan komunikasi (TIK) khususnya internet. Mereka sengaja masuk ke dalam *web* suatu instansi/lembaga tertentu kemudian melakukan kejahatan di dalamnya baik itu mencuri data ataupun mengacaukan data, bahkan tidak sedikit mencuri uang melalui internet seperti pembobolan nomor pin ATM. Kejahatan-kejahatan seperti inilah yang disebut sebagai *Cybercrime*. Masalah kejahatan dunia maya dewasa ini sepatutnya mendapat perhatian semua pihak secara seksama pada perkembangan teknologi informasi masa depan, karena kejahatan ini termasuk salah satu *extra ordinary crime* (kejahatan luar biasa) bahkan dirasakan pula sebagai *serious crime* (kejahatan serius) dan *transnational crime* (kejahatan antar negara) yang selalu mengancam kehidupan warga masyarakat bangsa dan negara berdaulat.

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

Banyak jenis dan ragam *cybercrime* salah satunya *phishing*. *Phishing* merupakan cara untuk mencoba mendapatkan informasi seperti *username*, *password*, dan rincian kartu kredit dengan menyamar sebagai entitas terpercaya dalam sebuah komunikasi elektronik. Komunikasi yang mengaku berasal dari populer situs *web* sosial, situs lelang, prosesor pembayaran *online* atau IT administrator biasanya digunakan untuk memikat publik tidak curiga. Informasi ini kemudian dimanfaatkan oleh pelaku kejahatan untuk mengakses rekening seseorang, menarik atau mentransfer sejumlah rekening ke pelaku, atau melakukan belanja *online* dengan menggunakan kartu kredit orang lain. Berbagai cara ditempuh untuk mewujudkan keinginan pelaku, yang paling sering adalah mengiming-imingi seseorang dengan hadiah, membuat *email* dan *website* palsu yang menyerupai *email* dan *website* bank yang asli. Ada beberapa tipe *phishing* yang kerap dilakukan oleh para pelaku kejahatan di dunia maya. Namun, jenis *phishing* yang paling populer dan kerap digunakan biasanya ada dua jenis. Yang pertama, adalah *clone phishing*. Pada *phishing* jenis ini, serangan dilakukan dengan melalui surat elektronik yang terlihat resmi dan mengandung *attachment* di dalamnya. *Attachment* ini kemudian digunakan untuk mengambil data dari korban untuk kemudian dikirimkan lagi ke tempat yang diinginkan oleh pelaku. Jenis yang kedua dinamakan *spear phishing*. Tingkat keberhasilan mencuri data pada jenis ini cenderung lebih tinggi karena si pelaku memiliki target yang lebih spesifik. Mereka mencari dan mengenali data dari targetnya terlebih dahulu sehingga korban tidak akan curiga bahwa dirinya sedang diserang. Data yang biasanya diambil bisa berupa *password*, nomor kartu kredit, nomor telepon, hingga nomor rekening bank yang biasanya dicantumkan korban pada layanan-layanan yang tersedia di internet seperti media *sosial*, *e-commerce*, penyimpanan *cloud*, sampai pinjaman *online*.

Penelitian ini merupakan penelitian analisis dimana tujuan penelitian ini untuk menginvetigasi dan menganalisis serangan *web phishing* dengan menggunakan metode *network forensic* dengan cara mengumpulkan semua *log* data. Digunakan metode *network forensic* dalam penelitian ini karena metode tersebut biasa digunakan untuk klasifikasi dokumen, deteksi *spam* atau *filtering spam*. Dan masalah klasifikasi lainnya. Kegunaan dari penelitian ini adalah membantu orang-orang untuk menemukan bentuk serangan dari *web phishing*.

Sekolah Menengah Kejuruan Swasta (SMKS) YP 17 Cilegon mempunyai beberapa program jurusan, diantaranya yaitu Teknik Komputer dan Jaringan (TKJ), Administrasi Perkantoran, Akuntansi, Penjualan/Pemasaran (Marketing), Perhotelan, Otomotif dan Teknik Kecantikan (TKK). Sekolah Menengah Kejuruan Swasta (SMKS) YP 17 Cilegon yang dipimpin oleh Ibu Kepala Sekolah Aan Suhanah pada tahun 2020 memiliki jumlah peserta didik sebanyak 1466 siswa yang tak lepas dari proses belajar mengajar menggunakan internet.

Oleh karena itu penelitian diarahkan untuk mendapatkan fakta-fakta yang berhubungan dengan aktivitas perlindungan teknologi informasi di lingkungan sekolah SMK YP 17 Cilegon serta mencegah terjadinya pencurian data. Selain itu peneliti juga menginginkan penelitian ini bisa menjadi proses pembelajaran bagi siswa/siswi di sekolah.

II. KAJIAN PUSTAKA

Dalam melakukan investigasi digital forensik perlu dikaji kebutuhan dan kesiapan infrastruktur yang menunjang (Charles dan Pollock, 2015). Metode NIST dapat digunakan untuk melakukan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital (Yudhana, 2018). Snort dapat memantau lalu lintas *packet* di dalam jaringan serta mampu mendeteksi serangan berdasarkan *rule* yang di-*set*, sehingga serangan jaringan komputer tersebut dapat segera ditangani segera mungkin oleh administrator karena terdapat *alert* (Dewi dan Kasih, 2017). Sumber serangan jaringan dapat ditentukan berdasarkan data log bukti, identifikasi, analisis, dan rekonstruksi kejadian (Aji dkk, 2017). Eksplorasi bukti digital pada *smart router* dapat menggunakan metode *live forensic* (Supriyono dkk, 2019).

Faiz dan Sidiq (2018) memberikan penjelasan secara detail dari apa saja yang dapat dicari, lokasi penyimpanan aktivitas *web browser*, format waktu yang digunakan sampai dengan *tools* untuk menginvestigasi aktivitas *web*. Mazdadi, dkk (2017) mengeksplorasi bagaimana caranya melakukan forensik perangkat Mikrotik berbasis RouterOS dan mengembangkan aplikasi jarak jauh untuk mengekstrak data router menggunakan API.

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".

Menurut Casey (2011) *Network forensics* adalah cabang pembantu forensik digital yang berkaitan dengan pemantauan dan analisis komputer lalu lintas jaringan untuk keperluan pengumpulan informasi, bukti hukum, atau deteksi intrusi.

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

"Sampai baru-baru ini, cukup melihat komputer individual sebagai objek terisolasi yang mengandung digital bukti. Komputasi berpusat pada disk mengumpulkan komputer dan beberapa disk akan memastikan koleksi semua bukti digital yang relevan. Namun, saat ini, komputasi telah menjadi berpusat pada jaringan karena semakin banyak orang bergantung pada *e-mail, e-commerce*, dan sumber daya jaringan lainnya. Tidak lagi memadai untuk memikirkan komputer isolasi karena banyak dari mereka yang terhubung bersama menggunakan berbagai teknologi jaringan. Digital peneliti/ pemeriksa harus menjadi ahli dalam mengikuti *cybertrail* untuk menemukan bukti digital terkait internet publik, jaringan pribadi, dan sistem komersial lainnya. Pemahaman tentang teknologi yang terlibat akan memungkinkan penyelidik digital untuk mengenali, mengumpulkan, melestarikan, memeriksa, dan menganalisis bukti terkait dengan kejahatan yang melibatkan jaringan."

Internet yang berisi jaringan forensik dan proses intersepsi yang sah menurut hukum adalah tugas-tugas yang penting untuk banyak organisasi termasuk *small medium business*, *enterprises*, industri *banking* dan *finance*, pemerintahan, forensik, dan agen intelijen untuk tujuan-tujuan yang berbeda-beda seperti penarsipan, intersepsi, dan mengaudit lalu lintas internet untuk referensi masa depan dan kebutuhan forensik. Pengarsipan ini dan pemulihan kembali data internet dapat digunakan untuk barang bukti hukum dalam beberapa kasus perselisihan. Pemerintah dan agen-agen intelijen mengunakan beberapa teknologi untuk melindungi dan mempertahankan keamanan nasional.

Dijelaskan dalam tiga komponen tahapan dalam menanganinya berupa:

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 aktifitas *phishing* secara *offline* dengan memanfaatkan berbagai *tools* (data *non-volatile*).
2. Analisis
   Kegiatan pada tahap ini yaitu mengamati secara detail data yang diperoleh dari proses *reconnaissance*, 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 dilakukan perbaikan sistem keamanan jaringan atau pemulihan kembali data yang telah hilang akibat adanya intrusi, khususnya informasi pada *disk* berupa *file* atau *directory.*

Tiga komponen dalam Digital *Forensic* dari bukti digital selanjutnya akan membahas hal yang sangat penting yaitu *Chain of Custody*. Menurut Cosic et al. (2011), *Chain of custody* adalah bagian penting dari proses investigasi yang akan menjaminkan suatu barang bukti dapat diterima dalam proses persidangan. *Chain of custody* akan mendokumentasikan hal terkait dengan *where, when, why, who, how* dari penggunaan barang bukti pada setiap tahap proses investigasi. Vacca (2005) mendefinisikan *Chain Of Custody* sebagai " *A Road Map That Shows how evidence was collected, analyzed and preserved in order to presented as evidence in court".*

Chain of Custody merupakan proses untuk merekam kronologi pengamanan, penahanan, pengendalian, dan pemindahan barang bukti fisik atau elektronik. *Chain of Custody* dituliskan dalam dalam sebuah dokumen yang berfungsi untuk menjelaskan kronologi penanganan barang bukti tersebut, sehingga diharapkan tidak menimbulkan keraguan pada saat proses pengadilan. Ketika barang bukti akan digunakan dalam proses pengadilan, maka diperlukan penanganan yang sangat hati-hati untuk mencegah terjadinya kontaminasi atau perubahan dari barang bukti tersebut. Ide dibalik *Chain of Custody* ini adalah untuk menegaskan bahwa barang bukti tersebut memang benar-benar terkait dengan tindak kejahatan, bukan semata barang bukti yang ditanamamkan di tempat kejahatan, hanya untuk membuat seseorang tampak bersalah.

Pihak yang berwenang harus selalu memiliki akses terhadap barang bukti, mendokumentasikannya, dan menyerahkannya kepada pihak yang bertanggung jawab terhadap *evidence room* (tempat pengamanan dimana barang bukti disimpan). Dokumen *Chain of Custody* tidak memiliki format yang standar atau baku, namun harus berisi informasi mengenai:

a. Barang bukti yang dikumpulkan.
b. Identitas semua penanggung jawab barang bukti.
c. Durasi penyimpanan barang bukti.

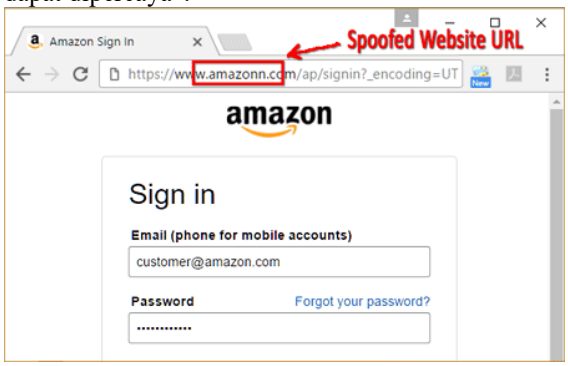
Pemindahan barang bukti termasuk di dalamnya adalah tanda tangan pihak yang terlibat dalam proses pemindahan barang bukti.

Web Pishing

Web phishing adalah situs *web* yang dirancang untuk melakukan bentuk penipuan dengan cara percobaan untuk mendapatkan informasi sensitif. Istilah *phishing* dalam bahasa Inggris berasal dari kata *fishing* alias memancing, dalam hal ini

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

maksudnya adalah memancing informasi dan kata. Dalam ruang lingkup keamanan komputer, *phishing* adalah salah bentuk kejahatan elektronik dalam bentuk penipuan. Dimana proses *phishing* ini bermaksud untuk menangkap informasi yang sangat sensitif seperti *username, password* dan detil kartu kredit dalam bentuk menyamar sebagai sebuah entitas yang dapat dipercaya/ *legitimate organization* dan biasanya berkomunikasi secara elektronik. *Phishing* diperkenalkan pertama kali pada tahun 1995. Menurut James (2005) cara pertama yang dilakukan *phisher* adalah dengan menggunakan algoritma yang membuat nomor kartu kredit secara acak. Jumlah kredit acak kartu yang digunakan untuk membuat rekening AOL. Akun tersebut kemudian digunakan untuk *spam* pengguna lain dan untuk berbagai hal lainnya. Program-program khusus seperti AOHell digunakan untuk menyederhanakan proses. Praktek ini diakhiri oleh AOL pada tahun 1995, ketika perusahaan membuat langkah-langkah keamanan untuk mencegah keberhasilan penggunaan angka kredit secara acak kartu. *Phishing* dikenal juga sebagai "*Brand spoofing*" atau "*Carding*" adalah sebuah bentuk layanan yang menipu dengan menjanjikan keabsahan dan keamanan *transfer* data yang dilakukan. Menurut Felten et al spoofing (1997) dapat didefinisikan sebagai "Teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah *host* yang dapat dipercaya".



Sumber : www.google.com

Gambar 1. Contoh *Web Phishing*

Sumber Sumber Ancaman Web *Phishing*

Untuk mengetahui sumber-sumber ancaman *phishing* penulis telah melakukan survei literatur *phishing* dengan membaca beberapa jurnal. Berikut adalah garis besar dari beberapa sumber ancaman *phishing* berdasarkan survei yang telah penulis lakukan:

a) *Email* berdasarkan survei yang telah dilakukan pada tahun 2014 ada lebih dari 120.000 serangan *phishing* yang berpuncak pada miliaran transmisi *email*. 65% dari serangan *phishing* mulai dengan mengunjungi *link* yang diterima dalam sebuah *email*. Pada Maret 2016, 229.265 laporan *email phishing* diterima oleh Kelompok Kerja Anti-*Phishing* dari konsumen. 18,3% penduduk Australia menjadi korban dari *phishing* melalui *email.*

b) *Website Phishing* pada *website* meliputi iklan dan sosial media (Facebook, Twitter, Instagram). Berdasarkan survei yang telah dilakukan Facebook memperkirakan 8,7% dari akun yang berjumlah 83.090.000 bukan milik pengguna yang sebenarnya dan perkiraan sekitar 1,5% (14.320.000) adalah akun yang secara tidak sengaja menyebarkan isi berbahaya tanpa diketahui oleh pengguna, seperti pesan spam dan *link* yang mencurigakan. Sebagian besar serangan *phishing* dilakukan melalui *web server* yang sudah di-*hack* dan 73% situs telah menjadi korban. Pada Maret 2016 123.555 situs *phishing* terdeteksi oleh Kelompok Kerja Anti-*Phishing*. 15,7% penduduk Australia menjadi korban *phishing* melalui situs belanja *online* dan 6,9% melalui sosial media.

c) *Malware Phishing* yang dilakukan melalui penyebaran *malwares* salah satunya adalah *malware Koobface* yang telah membuat 81% pengguna menjadi korbannya.

Cara Kerja *Phishing*

Berikut merupakan cara kerja *phishing* berdasarkan sumber-sumber ancaman *phishing*:

a) *Email*

Serangan ini dimulai dengan mengirimkan *email* yang terlihat dari sebuah organisasi yang kenal dengan korban. Kemudian *email* tersebut akan meminta mereka untuk memperbarui informasi mereka dengan mengikuti *link* URL yang terdapat dalam *email* tersebut. Pada dasarnya, *phishing* menggabungkan rekayasa sosial dan vektor serangan kompleks untuk menciptakan ilusi atau penipuan di mata penerima *email*. Penyerang akan mengirimkan jutaan *email* ke jutaan pengguna dan ribuan dari mereka setidaknya akan jatuh pada rekayasa tersebut. Pastinya serangan-serangan tersebut menggunakan *email* palsu untuk menipu pengguna untuk menipu pengguna agar mau membocorkan data pribadi.

b) *Website*

Pada situs *web* mereka akan diminta untuk memasukkan informasi rahasia pribadi, seperti dan nomor *password* rekening bank yang pada akhirnya akan digunakan untuk pencurian identitas. *Phiser* juga menggunakan *tool* untuk mencuri kode sumber laman *web* yang sah dan menggantinya dengan *web* palsu. Selain itu, *phiser* menciptakan *embedding link* untuk mendapatkan informasi sensitif milik korban.

c) Malware

Cara penyerangan dengan berpura-pura meminta karyawan untuk men-*download* suatu

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

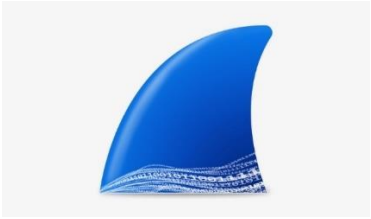
file yang dikirim oleh *phiser* sebagai penetralisir *malware* di komputer nantinya.

d) Trojan hosts
Phiser mencoba *login* ke *account* pengguna untuk mengumpulkan kredensial melalui mesin lokal. Informasi yang diperoleh kemudian dikirim ke *phisher*.

e) 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.

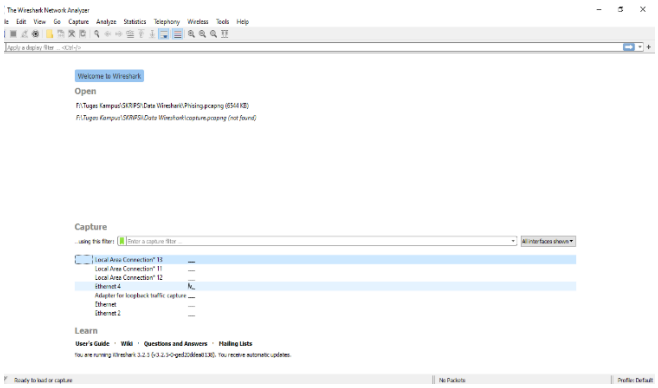
Wireshark

Wireshark yaitu *Network Protocol Analyzer*, termasuk juga ke dalam satu diantara *network analysis tool* atau *packet sniffer*. *Wireshark* mengizinkan pengguna mengamati data dari jaringan yang tengah beroperasi atau dari data yang ada di *disk*, dan segera melihat/mensortir data yang tertangkap, mulai dari informasi singkat dan rincian untuk segala hal tentang paket termasuk juga *full header* & jumlah data, bisa didapat. Sebenarnya *Wireshark* tidak didesain untuk *hacker*. *Wireshark* utamanya dibuat untuk *Administrator* Jaringan untuk dapat melacak apa yang terjadi di dalam jaringan miliknya atau untuk memastikan jaringannya bekerja dengan baik, serta tidak ada yang melakukan hal-hal buruk pada jaringan itu. *Wireshark* mempunyai sekian banyak *feature* termasuk juga *display filter language* yang banyak dan kapabilitas mereka dalam satu aliran pada sesi TCP. Paket *sniffer* sendiri diambil kesimpulan sebagai satu buah *tool* yang berkemampuan menahan dan melakukan pencatatan pada *traffic* data dalam jaringan. Pada saat jalan aliran data dalam jaringan, *packet sniffer* bisa menangkap *protocol* data unit (PDU), lakukan *decoding* juga analisis pada isi paket. *Wireshark* sebagai satu diantara *packet sniffer* yang diprogram sedemikian rupa agar mengetahui berbagai macam bentuk protokol jaringan. *Wireshark* juga dapat mendatangkan hasil enkapsulasi dan *field* yang ada di dalam PDU.



Sumber: https://www.pngkit.com/view/u2e6w7t4u2i1o0e6_wireshark-icon/

Gambar 2. *Wireshark Icon*



Sumber : Data Pribadi

Gambar 3. Wireshark GUI

Mikrotik

Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer berperan sebagai *network* (jaringan), pengendali, atau pengatur lalu lintas antar jaringan. Komputer jenis ini disebut dengan *Router*. Dimana *router* ini merupakan media penghubung dan pengatur antara dua buah jaringan atau lebih yang berguna dalam meneruskan data dari satu jaringan ke jaringan lainnya. Dengan demikian mikrotik bisa diartikan sebagai sistem operasi *router* yang digunakan untuk menjalankan dan mengatur segala aktivitas *network* (jaringan) secara menyeluruh. Router mikrotik bisa digunakan pada jaringan komputer berskala besar maupun kecil yang tentunya harus disesuaikan dengan *resources* daripada komputer itu sendiri. Jika mikrotik digunakan untuk mengatur *network* kecil, maka penggunaan perangkat komputernya bisa biasa-biasa saja atau standar, namun untuk skala besar maka harus menggunakan komputer yang memiliki spesifikasi tinggi. Mikrotik meliputi beragam fitur yang diciptakan untuk jaringan *wireless* dan *IP network*. Sistem ini cocok digunakan oleh *ISP*, *provider hotspot* dan warnet. Mikrotik seringkali disebut sebagai Router OS yang memiliki fungsi yang handal dan punya banyak sekali fitur yang mendukung kelancaran *network*. Mikrotik didesain agar mudah digunakan, baik untuk urusan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem, baik skala kecil hingga rumit sekalipun.

Sumber : http://www.mikrotik.co.id/produk_lihat.php?id=194

Gambar 4. Router mikrotik rb750

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

Komponen Jaringan

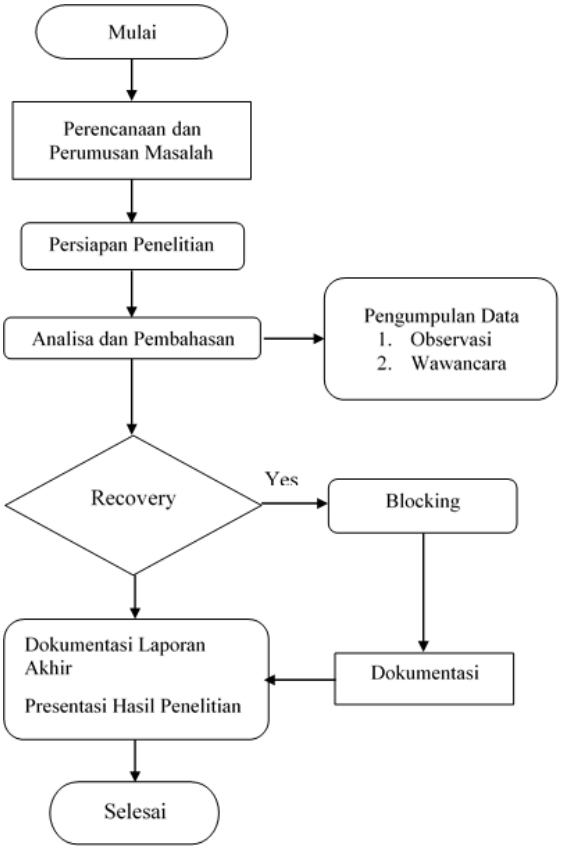
Beberapa jenis peralatan menurut Volonino dan Anzaldua (2008) untuk memahami bagaimana *system forensic* bekerja pada jaringan yang telah dilakukan untuk tingkat besar, adalah:

1. *Host*; setipe perangkat komputasi yang terpasang ke jaringan memiliki alamat IP dan alamat MAC. *Computer* adalah sebuah *host* yang memiliki alamat IP dan alamat MAC, juga laptop, PDA, WAP, router, *Switch*, maupun perangkat *mobile* seperti *smartphone*, ipod juga telah memiliki alamat IP dan MAC.
2. Router: sebuah *Computer* khusus yang bertujuan memindahkan data yang melintasi dua jaringan *IP address* ang berbeda. Router bekerja pada lapisan tiga dalam model OSI.
3. *Switch*: *Computer* jaringan yang menggunakan *Media Access Control* (MAC) identifikasi dari sebuah *Host* pada jaringan untuk memindahkan data dalam jaringan. *Switch* bekerja pada lapisan tiga dalam model OSI yang merupakan penghubung jaringan *multiport* untuk menembatani segmen jaringan.
4. *Hub*: perangkat jaringan yang beroperasi di *OSI layer 1*. *Physical Layer*. Perangkat tersebut sebagai penyambung atau *concentrator*, dan menguatkan sinyal di kabel *UTP*. Menggunakan *Hub* dapat mengalami *collision* karena *Hub* tidak dapat mengenal *MAC Address / Physical Address* yang mengakibatkan tidak dapat memilah data yang akan ditransmisikan. Sekarang *Hub* jarang digunakan karena cenderung meningkatkan *volume traffic* dan memeperlambat jaringan sedangkan *Switch* jauh lebih efisien dalam memindahkan data.
5. *Network Interface Card* (*NIC*): perangkat keras yang berbentuk kartu dengan kegunaan untuk menjadi jembatan komputer ke sebuah jaringan komputer. Cara kerjanya mengubah aliran data paralel dalam bus komputer menjadi bentuk data serial yang dapat ditransmisikan ke dalam media jaringan.
6. Media: sebuah bagian dari jaringan yang dapat berbentuk kabel tembaga, kabel serat *optic* atau gelombang radio. Memungkinkan untuk menghubungkan perangkat ke jaringan dan media yang berbeda juga protokol yang berbeda untuk membantu menciptakan rentang waktu dan data yang dapat mengaitkan tersangka.

III. METODE PENELITIAN

Tahapan Penelitian

Tahapan penelitian mencangkup langkah-langkah pelaksanaan dari awal sampai akhir, adapun langkahnya sebagai berikut:



Gambar 5. Tahapan Penelitian

Alat dan Bahan Penelitian

Perangkat keras yang digunakan pada penelitian ini 1 unit laptop Acer type Aspire E 14 dengan spesifikasi seperti ditampilkan pada Tabel 1.

Tabel 1. *Spesifikasi Hardware* yang Digunakan

No	Item	Deskripsi
1.	Processor	Intel Core i3 2.0 Ghz
2.	Memory	4 GB
3.	Hardisk	1 TB
4.	Modem Huawei	E5673
5.	Router Mikrotik	Rb941

Perangkat Lunak yang digunakan pada penelitian ini ditampilkan pada Tabel 2.

Tabel 2. *Spesifikasi Software* yang Digunakan

No	Item	Deskripsi
1.	Google Chrome	V.3.2.2
2.	WireShark	V.80.0.3987.149
3.	Winbox	V.3.18

Selain dari itu terdapat beberapa web yang digunakan dalam menganalisis aktifitas *phishing* seperti ditampilkan pada tabel 3.

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

Tabel 3. URL Pemeriksaan *Web Phishing*

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

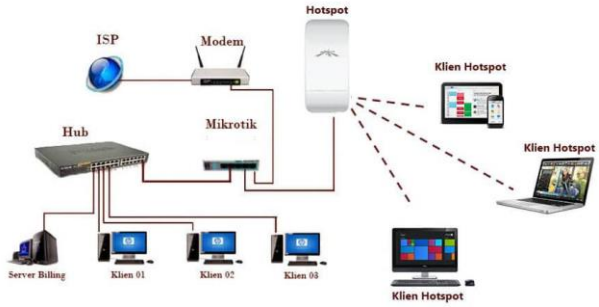
Data Penelitian

Yang dimaksud dengan sumber data dalam penelitian adalah subjek darimana data dapat diperoleh. Sumber data penelitian dapat bersumber dari data primer dan data sekunder.

1. Data Primer Sumber data yang langsung memberikan data kepada pengumpul data. Sumber data primer dalam penelitian ini adalah siswa/siswi dan guru di sekolah. Adapun data yang diperoleh adalah hasil laporan adanya beberapa *web phishing*.
2. Data Sekunder Sumber yang tidak langsung memberikan data kepada pengumpul data. Sumber data sekunder dalam penelitian ini adalah:
   a. struktur jaringan
   b. komponen yang digunakan
   c. serta tingkat keamanan jaringan yang ada di sekolah.

Topologi Jaringan

Topologi yang akan dibangun tetap menggunakan topologi yang sudah ada dan tidak merubah rangkaian yang sudah terpasang sebelumnya. Berikut ini gambaran topologi yang meliputi keseluruhan rangkaian pada di SMK YP 17 Cilegon.



Sumber : https://www.decisionsonevidence.com/cara-setting-dhcp-server-dan-dhcp-client-pada-router-mikrotik/

Gambar 6. Model Rancangan

Rancangan Pengujian

Pada tahap pengujian, penulis akan melakukan pengujian pada sebuah *website* apakah benar terjadi adanya *phishing* berdasarkan hasil dari laporan beberapa orang. Pengujian akan dilakukan meliputi akuisisi dan pengintaian, analisis, *recovery.*

Collection

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 aktifitas *phishing* secara *offline* dengan memanfaatkan berbagai *tools* (data *non-volatile*). Pada tahap ini *collection* data dilakukan secara *offline*. Data non-volatile yang berhasil dikumpulkan pada tahap ini, diperoleh laporan dari beberapa orang yang melaporkan bahwa adanya *phishing*.

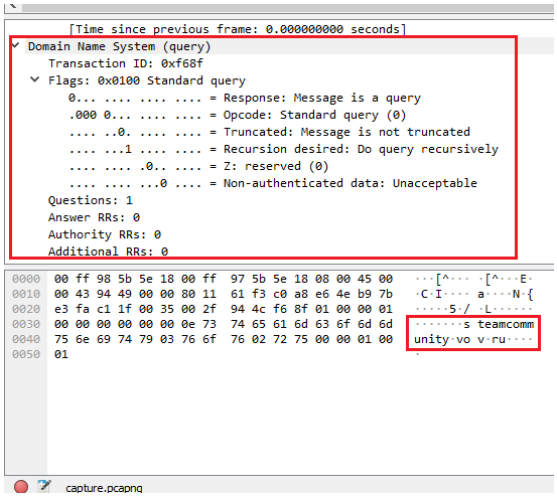
Analisis

Kegiatan pada tahap ini yaitu mengamati secara detail data yang diperoleh dari proses *reconnaissance*, dengan cara menguraikan komponen-komponen pembentuknya atau penyusunnya untuk dikaji lebih lanjut. Proses investigasi dan analisis dilakukan pada *website* yang diduga adanya *phishing*. Proses investigasi dan analisis *file* *.pcap dilakukan menggunakan perangkat lunak *wireshark*, sehingga diperoleh investigasi yang dilakukan berupa pencarian informasi: URL yang terlibat dalam aktifitas *phishing*, *IP address*, identitas penyerang (*phiser*), pencarian waktu dan tanggal serangan, network protocol (ICMP, TCP, UDP), DNS, FTP, SMTP, HTTP.

File Capture Phishing

Paket data ini adalah sebuah *query request* kepada DNS *Server*. Ini 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 System* (*query*), hasilnya seperti ditampilkan pada gambar 6.

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

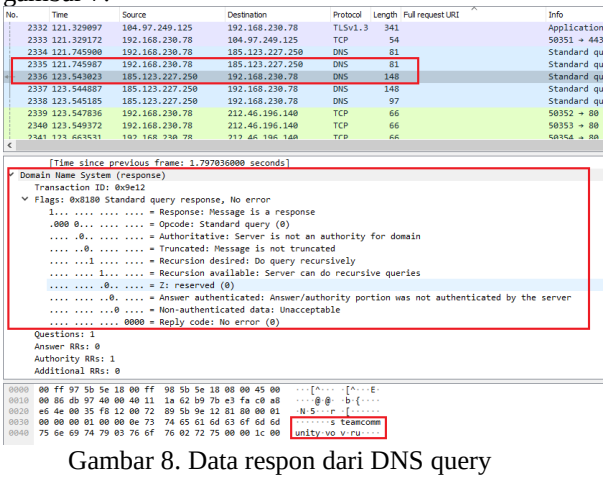


Gambar 7. Data respon dari DNS query

Gambar 6 menampilkan *format header* pada paket data yang berisi informasi protokol DNS. Diketahui bahwa aktifitas tersebut melakukan *query* terhadap domain http://steamcommunity.vov.ru/. Analisis terdapat *query* tersebut sebagai berikut:

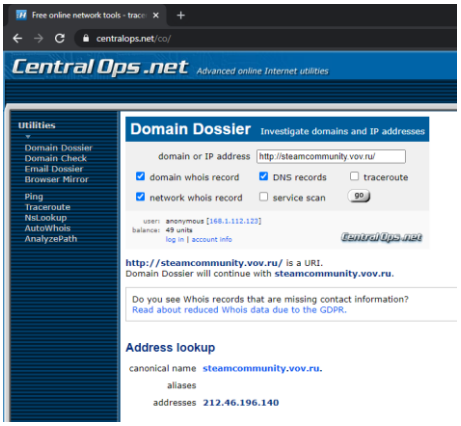
1. *Flags* bernilai 0x0100, memiliki arti:
   a. QR bernilai 0 berupa query.
   b. X menunukan nilai Opcode 000 yaitu berupa query.
   c. TC bernilai 0 artinya *Not Truncated*.
   d. RD bernilai 1 artinya *Rercursion not desired*.
   e. AA bernilai 0 artinya *Not Authoritative*.
2. Question RRs bernilai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

Selanjutnya untuk melihat respon dari paket data, klik paket data maka akan diperoleh hasil *format header* DNS seperti ditampilkan pada gambar 7.



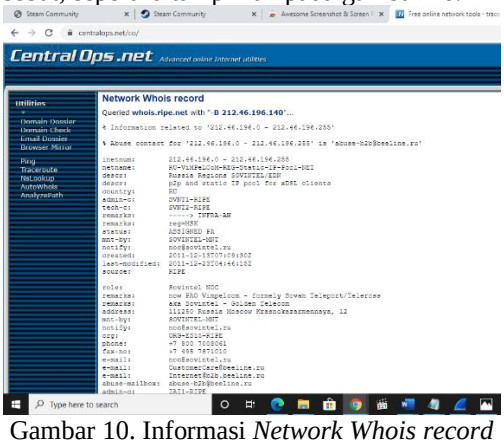
Gambar 8. Data respon dari DNS query

Gambar 8 menampilkan informasi detail hasil respon paket data. Diketahui bahwa respon DNS *query* http://steamcommunity.vov.ru/ dengan *IP address source* 192.168.230.78 dan *IP address destination* 185.123.227.250. Dengan hasil analisis protokol DNS sudah diketahui DNS yang digunakan oleh *phiser* dalam melakukan serangan sehingga disimpulkan untuk file *phishing*.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 http://steamcommunity.vov.ru/ pada kolom pencarian domain, maka diperoleh informasi seperti ditampilkan pada gambar 9.



Gambar 9. Informasi IP Address domain http://steamcommunity.vov.ru/ hasil DNSLookup

Gambar 9 menampilkan informasi, *domain* http://steamcommunity.vov.ru/ menggunakan *server* dengan *IP Address* 212.46.196.140. Bila tampilan informasi pada *web* seperti ditampilkan pada gambar 8 digeser ke bawah, maka akan diperoleh informasi lainnya, mengenai domain tersebut, seperti ditampilkan pada gambar 10.



Gambar 10. Informasi *Network Whois record* domain http://steamcommunity.vov.ru/ hasil DNSLookup

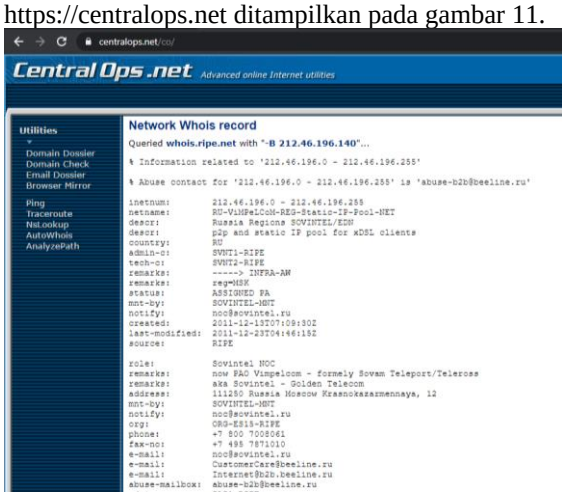
Gambar 10 menampilkan informasi *Network Whois record* yang berhubungan dengan domain http://steamcommunity.vov.ru/. Dari data tersebut, diperoleh beberapa informasi penting diantranya:

a. Nama pendaftar domain: *Private Person*

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

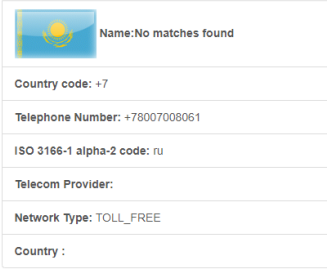
b. Alamat : 111250 Russia Moscow, Krasnokazarmennaya, 12
c. Negara : Rusia
d. Telp. : +7 800 7008061 & +7 495 7871000
e. Tgl. Dibuat : 13-12-2011
f. *e-mail* : noc@sovintel.ru

Pemeriksaan lebih lanjut mengenai informasi *URL phishing* dilakukan terhadap *domain* .vov.ru dengan sengaja dibuat satu *domain* baru menggunakan vov.ru. yaitu amper.vov.ru. Hasil *dnslookup domain* amper.vov.ru melalui https://centralops.net ditampilkan pada gambar 11.



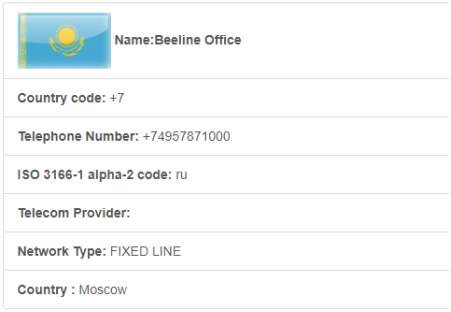
Gambar 11. DNSLookup URL www.amper.vov.ru

Gambar 11 menampilkan informasi web www.amper.vov.ru yang sengaja dibuat dengan domain .vov.ru. Setelah dibandingkan informasi nslookup dengan web http://steamcommunity.vov.ru/ 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 Private Person bukanlah nama pendaftar domain http://steamcommunity.vov.ru/ tetapi pemilik hosting untuk domain vov.ru. Pemeriksaan lebih detail mengenai data *source* hasil dnslookup dilakukan pada identitas data phone. Investigasi dilakukan dengan bantuan fasilitas yang tersedia di web www.emobiletracker.com. Informasi hasil pencarian berdasarkan data *phone* dan lokasi ditampilkan pada gambar 12.



Gambar 12. Informasi Data Person Berdasarakan Data *Phone* +7 800 7008061

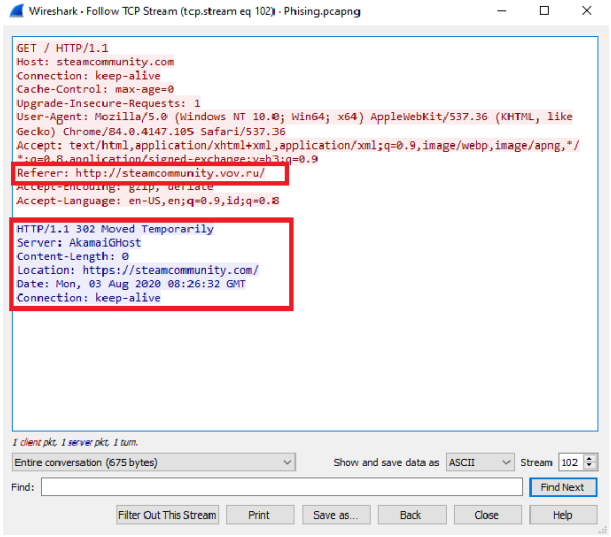
Gambar 12 menampilkan hasil pencarian dengan parameter data *phone* dan lokasi, bahwa dari data source tersebut nomor *handphone* tidak terdaftar. Berbeda dengan nomor *telephone* +7 495 7871000 yang ditampilkan pada gambar 13.



Gambar 13. Informasi Data Person Berdasarakan Data Phone +7 495 7871000

Gambar 13 menampilkan hasil pencarian dengan parameter data phone dan lokasi bahwa dari data *source* tersebut nomor *handphone* terdaftar dengan pemilik bernama Beeline Office. Informasi yang ditunjukan berbeda dengan hasil data *source* dnslookup.

Selanjutnya pada *File phishing*.pcap menyimpan informasi dari paket data. Informasi yang tersimpan dalam paket data ini berkaitan dengan protokol TCP, TSLv1 dan HTTP. Pada paket data nomor 3213, ditampilkan protokol TLSv1 dengan melakukan TCP *stream* ke sebuah *link* menuju *website* www.steamcommunity.com dengan *IP Address Source* 192.168.230.78 dan *IP Address Destination* 104.97.249.125. Paket data nomor 3213 dengan protokol HTTP terdapat perintah HTTP/1.1 302 *Moved Temporarily*, kode ini mengubah jenis permintaan menjadi GET tanpa memedulikan bentuk aslinya dan 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 14.



Gambar 14. Isi paket data nomor 3213

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

Gambar 14 menampilkan infomasi *request* dengan metode GET dari suatu klien ke domain www.steamcommunity.com.

Rancangan *Recovery*

Pada tahap ini, sistem keamanan jaringan akan di-*recovery* menggunakan router mikrotik yang akan dikonfigurasi untuk *membloking website* yang sudah terbukti adanya *phishing.*

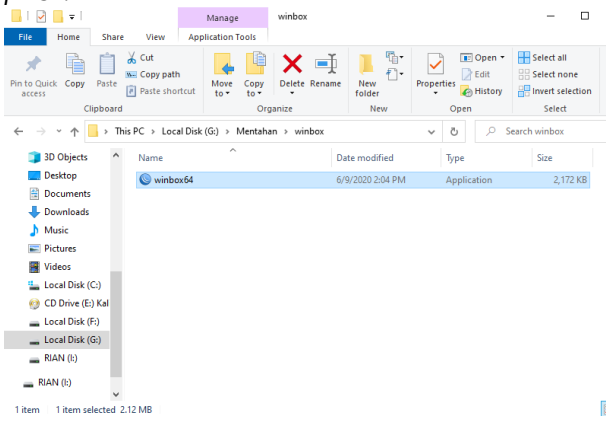
1. Konfigurasi Dasar

Pada tahap ini, yang dilakukan ialah melakukan konfigurasi pada *interface* yang digunakan sebagai jalur keluar masuk internet lewat *router mikrotik* dengan cara memberikan nama agar mudah dipahami ketika melakukan konfigurasi. Kemudian, menetapkan koneksi ISP dan melakukan permintaan alamat IP (DHCP). Selanjutnya, melakukan konfigurasi *IP Address* pada masing masing *Ethernet* dan DNS yang akan digunakan.

2. Konfigurasi *Blocking Web*

Rancangan instalasi ini menggambarkan alur dari proses blocking situs yang akan dilakukan. Dari koneksi internet Telkom Indonesia melalui modem dihubungkan ke mikrotik rb750 diteruskan ke PC.

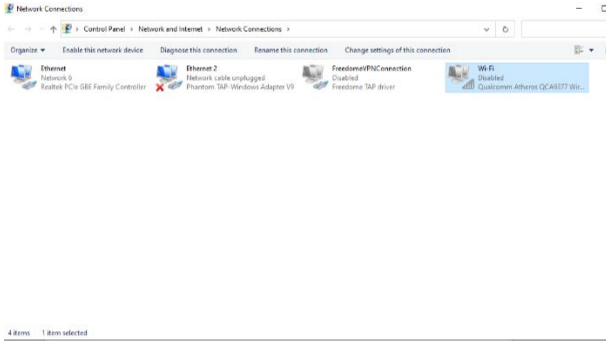
Instalasi Mikrotik Dengan Winbox Adapun langkah instalasi mikrotik pada winbox yaitu jalankan *file* winbox.exe kemudian next sampai *finish.*



Gambar 15. *Software Winbox*

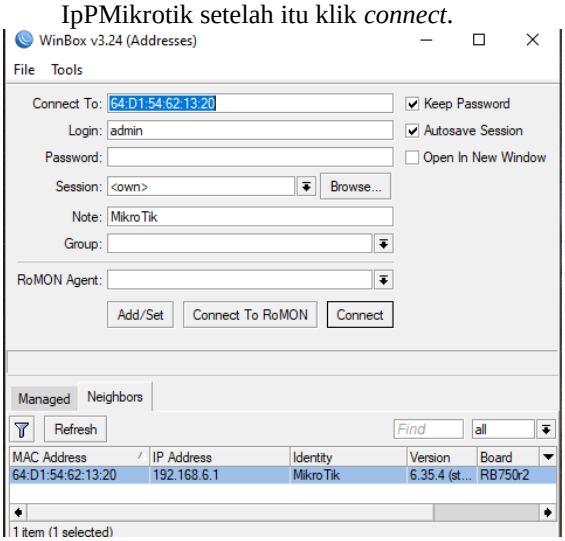
Lalu seting mikrotik:

1. Pastikan *Wireless Network Connection* PC dalam keadaan *disabled.*



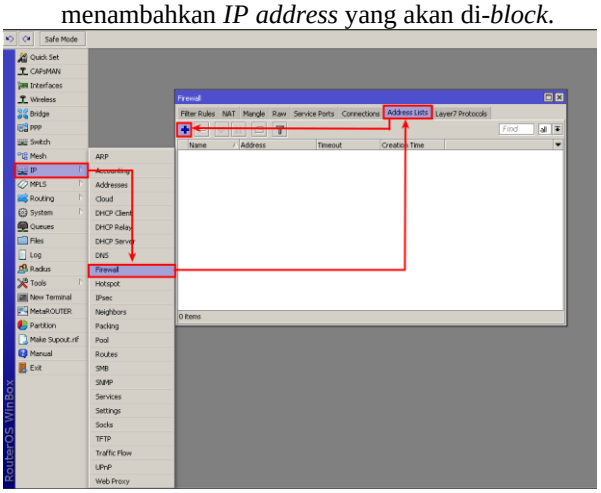
Gambar 16. *Adapter Option Connection*

2. Buka aplikasi winbox kemudian, masukkan IpPMikrotik setelah itu klik *connect.*



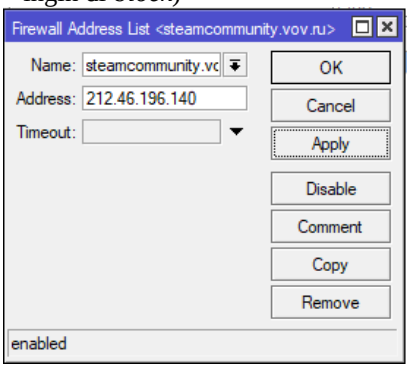
Gambar 17. Tampilan Aplikasi Winbox

3. Setelah berhasil *connect*, lalu masuk ke *Address List* dengan **IP>Firewall>Address List>Klik Add atau tombol (+)**, untuk menambahkan *IP address* yang akan di-*block.*



Gambar 18. *Setting Address List*

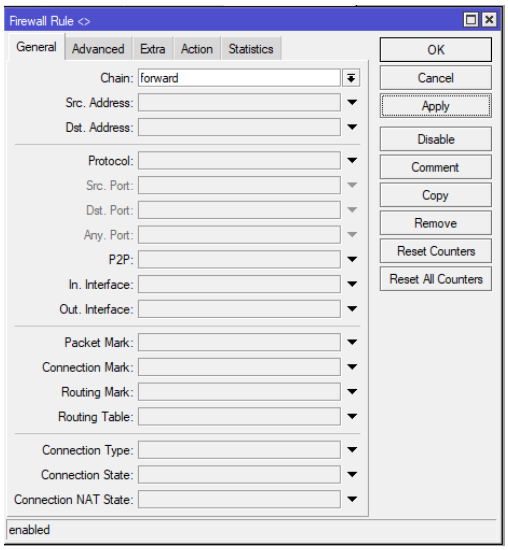
4. Kemudian Isikan:
   a. Name = steamcommunity.vov.ru (Untuk memberi nama identitas suatu situs yang ingin di-*block*)
   b. Address = 212.46.196.40 (Alamat IP yang ingin di-*block*)



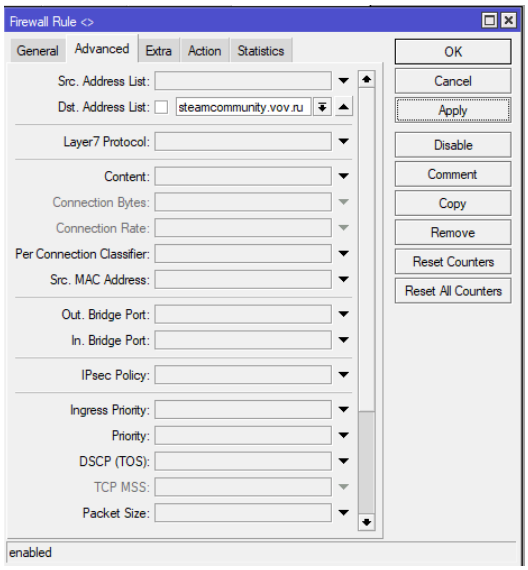
Gambar 19. List *website* yang akan di blokir

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

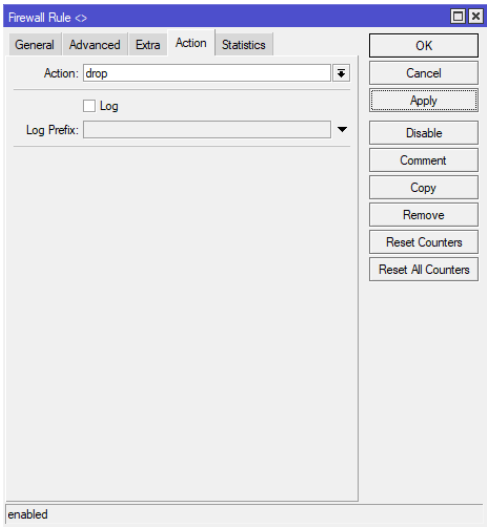
5. Setelah itu pindah ke *tab Filter Rules*, kemudian klik tanda +,
   a. pada tab *General*, isikan *Chain = Forward*
   b. pada tab *Advanced*, isikan Dst.Address List = steamcommunity.vov.ru (*Address list* yang dibuat tadi)
   c. pada tab *Action*, isikan *Action = Drop*



Gambar 20. *Tab General*



Gambar 21. *Tab Advanced*



Gambar 22. *Tab Action*

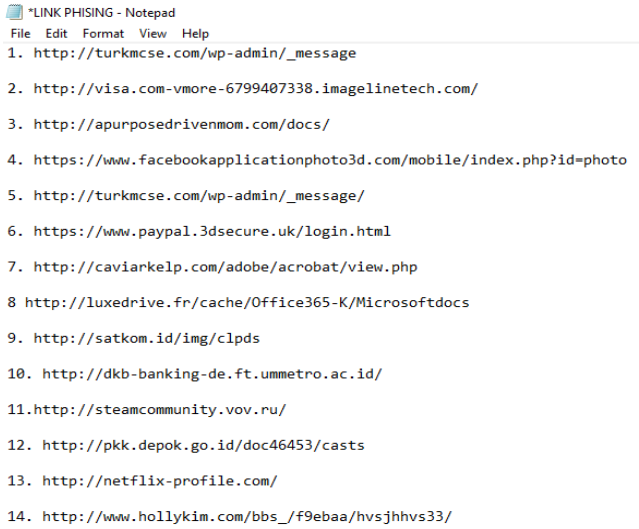
IV. HASIL DAN PEMBAHASAN

Hasil Penelitian

Setelah melakukan perancangan dan melalui tahap pengujian sistem yang dibangun, maka didapatkan beberapa hasil yang didapat dalam bentuk visualisasi data. Data yang ditunjukkan dalam penulisan ini, yaitu berupa tangkapan layar monitor dari analisis *web phishing* dengan metode *network forensic*.

Hasil *Collection*

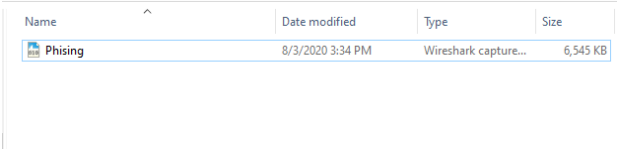
Pengumpulan data dapat dilakukan dengan dua cara yaitu: pengumpulan data dengan bekerja pada sistem *online* (data volatile) dan pengumpulan data dari *disk* yang terkait dengan aktifitas *phishing* secara *offline* dengan memanfaatkan berbagai *tools* (*data non-volatile*), maka diperoleh 14 *link web* yang diduga *phishing*, pada gambar 23 berikut yang telah berhasil dikumpulkan.



Gambar 23. *Link Phishing*

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

Dari data yang berhasil dikumpulkan, penulis menganalisis sebuah *website* pada nomor 11 yaitu http://steamcommunity.vov.ru/. Selanjutnya dilakukan proses investigasi dan analisis dilakukan pada *website* yang diduga adanya *phishing* dan menghasilkan sebuah *file capture* seperti pada gambar 24.



Gambar 24. Hasil investigasi dan analisis menggunakan wireshark

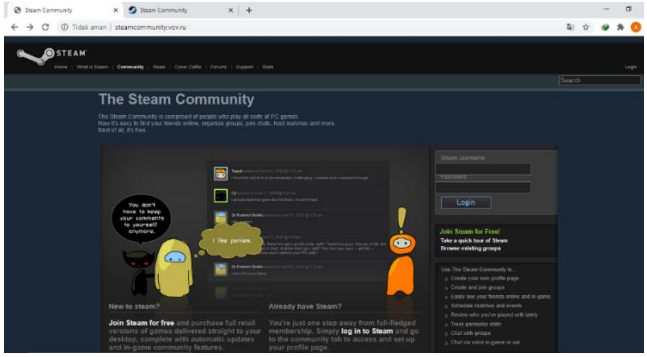
Hasil Analisis *Web*

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, berikut hasilnya:

1. Protokol DNS (*Domain Name System*)
   a. Host *Phishing* http://steamcommunity.vov.ru/
   b. IP address Source = 192.168.230.78
   c. IP Destination = 185.123.227.250
   d. User-Agent = Mozilla/5.0
   e. Server Apache/1.3.27 (Unix) (Redhat/Linux)
   f. Person Domain = Dimitar Dimitrov
   g. Address = Rusia
   h. Create = 2011-12-13T07:09:30Z
2. Protokol HTTP (Hypertext Transfer Protokol)
   a. Host : steamcommunity.com
   b. Connection : keep-alive
   c. User Agent : Mozilla/5.0
   d. Accept : text/html
   e. Referer : http:steamcommunity.vov.ru
   f. Accept-Encoding : gzip, deflate
   g. Accept-Language : en-US
   h. Date : Mon, 03 Aug 2020 08:26:32 GMT

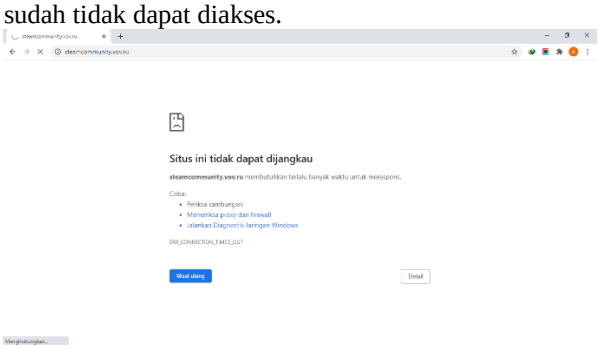
Hasil *Recovery*

Setelah melakukan proses *recovery* pada sistem keamanan jaringan, maka pada Gambar 25 ditampilkan situs steamcommunity.vov.ru sebelum diblokir.



Gambar 25. Tampilan situs steamcommunity.vov.ru sebelum diblokir

Dari hasil yang didapat setelah melakukan konfigurasi mikrotik untuk memblokir situs web Pada Gambar 26 ditampilkan hasil dari pemblokiran situs steamcommunity.vov.ru bahwa situs *phishing* sudah tidak dapat diakses.



Gambar 26. Tampilan situs steamcommunity.vov.ru setelah diblokir

Pembahasan Penelitian

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 berikut:

1. Pada proses analisis menggunakan *tools wireshark*, dapat disimpulkan bahwa aktivitas yang tidak wajar, Diketahui bahwa respon DNS *query* http://steamcommunity.vov.ru/ dengan *IP address source* 192.168.230.78 dan *IP address destination* 185.123.227.250 Hasil penelitian ini juga berhasil mengidentifikasi IP Address List dari penyerang, yaitu IP 192.168.230.78.
2. Pada tanggal 13-12-2011 telah dibuat suatu host *phishing* http://steamcommunity.vov.ru/. Berdasarkan hasil investigasi, domain vov.ru terdaftar atas nama: Private Person yang berlokasi di Rusia.
3. Informasi yang ditunjukan pada informasi data person berdasarkan data phone terdaftar dengan nama Beeline Office berbeda dengan hasil data source dnslookup, namun data mengenai lokasi sama.

Dari hasil proses recovery sistem keamanan jaringan, sistem *blocking* menggunakan router mikrotik telah mampu melakukan blokir pada *website phishing* dengan baik sehingga weh *phishing* tidak dapat diakses.

V. PENUTUP

Kesimpulan

Kesimpulan yang didapatkan setelah melakukan penelitian adalah:

1. Terdapat 3 langkah dalam investigasi *network forensic*, diantaranya yaitu Akuisisi dan pengintaian, Analisis, *Recovery*. Hasil pada tahap akuisisi dan pengintaian ditemukan 14 *web* yang diduga *phishing*, pada tahap analisis pengecekan dilakukan pada sebuah web

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

dengan url http://steamcommunity.vov.ru, dan pada tahap *recovery* berhasil melakukan *blocking* pada *website* tersebut.

2. Untuk merancang sistem mendeteksi dan memblokir *web phishing* diperlukan perangkat sebagai berikut:
   a. *Hardware*: Processor, Memory, Hardisk, Modem, dan Router.
   b. *Software*: Google Chrome, Wireshark dan Winbox
3. Dengan menambahkan router mikrotik pada rancang bangun jaringan, *user* akan aman dari ancaman *web phishing* sehingga dapat mencegah terjadinya pencurian data.

Saran

Berikut adalah saran mengenai pengembangan untuk penelitian selanjutnya:

1. Menggunakan lebih banyak *tools* untuk mengetahui informasi lebih detail terkait identitas yang terlibat dalam aktifitas *phishing.*
2. Dapat membuat aplikasi atau alat untuk memberi peringatan.

DAFTAR PUSTAKA

Dwi, Tayomi et al. (2017). "Analisis *Live Forensics* Untuk Perbandingan Aplikasi Instant Messenger pada Sistem Operasi Windows 10". Institut Teknologi Sepuluh Nopember: Undergraduate thesis.

Faiz, M.N., Umar, R., dan Yudhana, A. (2016). "Analisis *Live Forensic* Untuk Perbandingan Keamanan *Email* Pada Sistem Operasi *Proprietary", Jurnal Ilmiah ILKOM* Vol. 8, No. (3)

Faiz, M.N., Umar, R., dan Yudhana, A. (2016). "Implementasi *Live Forensics* untuk Perbandingan *Browser* pada Keamanan *Email", Jurnal JISKA*, Vol. 1, No. (3)

Vidila, R., Andri, S., Natsir. (2016). "Analisis Data *Recovery* Menggunakan *Software Forensic: Winhex and X-Ways Forensic*", *Jurnal* PROSISKO, Vol. 3, No. (1)

Fletcher, David, (2015). "*Forensic Timeline Analysis using Wireshark GIAC (GCFA) Gold Certification"*. SANS Institute InfoSec Reading Room.

Ginanjar, A. dkk, (2018) "Analisis Serangan Web *Phishing* pada Layanan E-commerce dengan Metode Network Forensic Process" *jurnal JUTEI* Vol.2, No.(2)

Gulshan (2016). "*Network Forensics: Methodical Literature Review"*. Galgotias: University India.

Lazzez, A. Slimani T (2015). *Forensic Investigasion of Web Application Security Attacks*. J Computer Network and Information Security.

Lumanto, R. (2016). "*Internet Protection & Safety"*. Batam : APJII Open Policy Meeting.

Sharma, Kavita. dkk. (2016). "*Network Forensics: Today and Tomorrow"*. Galgotias : University,India

(2013, Juni 24) Retrieved Agustus 10, 2020, From Suharno jaya. "forensic digital document" : https://suharnojaya.wordpress.com/2013/06/24/konsep-ontologi-untuk-chain-of-custody-2/

Sunardi, Riadi, I., Nasrulloh I.M. (2019). "Analisis Forensik *Solid State Drive (SSD)* Menggunakan *Framework GRR Rapid Response", Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)* Vol. 6, No. (5)

Wahyudi, A dan Cahyono, B. S. (2016). "Sistem Keamana dan Optimalisasi Bandwith Menggunakan Mikrotik RB750 Di PT Pupuk Kaltim". Bontang : Universitas Islam Indonesia.