JURNAL TIMES
TECHNOLOGY INFORMATICS & COMPUTER SYSTEM

Volume XII No 1, Juni 2023
*p*ISSN : 2337 – 3601
*e*ISSN : 2549 – 015X

Tersedia *online* di http://ejournal.stmik-time.ac.id

ANALISA HASIL CAPTURE KEGIATAN ILEGAL DI DALAM JARINGAN MENGGUNAKAN WIRESHARK

Achmad Firly Henry Egitha
Jurusan Teknik Informatika
Universitas Muhammadiyah Sidoarjo
Jl. Raya Gelam 250 Candi Sidoarjo
email: achmadfirly2@gmail.com

Abstrak

Dalam sebuah keamanan jaringan komputer sering terjadi kegiatan legan dan ilegal yang sudah menjadi hal yang sudah mutlak. Hal ini dipengaruhi oleh pola fikir pengguna jaringan komputer. Pada dasarnya sistem keamanan yang sudah terinstall pada sebuah komputer hanya memberikan layanan dalam bentuk standart atau default sehingga dalam menyeimbangkan kebutukan keamanan perlu adanya adaptasi terhadap sistem keamanan jaringan komputer. Untuk memenuhi kebutuhan keamanan jaringan komputer perlu tools pendukung yang mampu melakukan fungsi filterjaringan komputer agar bisa menangkap hasil kegiatan ilegal atau kegiatan yanng bersifat negatif. Ada beberapa jeniskegiatan ilegal yang sering dilakukan yang melibatkan pengguna dengan jaringan komputer seperti tindakan hacking,pencurian data, melakukan pencarian yang bersifat negatif. Dari jenis kegiatan tadi memiliki tujuan yang sama yakni untuk mencapai tujuan dengan hal ilegal. Tools yang digunakan dalam menangkap hasil pencarian jaringan komputercukup banyak jenisnya tergantung fitur yang tersedia, namun dalam kasus ini penulis menggunakan software Wireshark untuk mendapatkan hasil capture kegiatan ilegal dalam jaringan komputer yang akan terjadi sehingga lalu lintas jaringan komputer tetap bersifat positif.

Kata Kunci: Capture, Kegiatan Ilegal, Jaringan Komputer, Wireshark

1. Pendahuluan

Sebuah keamanan jaringan komputer merupakansuatu hal yang penting dalam sistem komputer agar terhindar dari kegiatan negatif. Dalam kasus ini akanmencoba kegiatan ilegal dan cara menangkap hasil kegiatan tersebut yaitu dengan cara menangkap hasilkegiatan ilegal didalam jaringan komputer lalumenangkap hasil kegiatan ilegal tersebut. Dalam halini tedapat 2 sistem komputer yang melibatkan sistemkeamanan yaitu hardware dan software. Hardwaremelibatkan device dan software melibatkan tools yangdigunakan masing-masing pengguna. Pelaku kegiatanilegal dalam melakukan aksinya dipastikan memilikitujuan dan maksud yang telah dirancang secarasistematis guna mengurangi nilai kegagalan atau tidakmendapat hasil yang diinginkan pelaku kegiatan ilegal.Pada dasarnya sistem keamanan jaringan dengan status default sudah menyediakan fitur-fitur yangsering digunakan dalam menjaga keamanan jaringankomputer itu sendiri, namun dalam kasus lain ada 2 jenis metode yang digunakan yaitu sistem pendeteksikegiatan ilegal atau sering disebut security sistem danadapun juga search record atau rekaman pencarian yang berbentuk file cache.

Software Wireshark merupakan aplikkasi yang berfungsi untuk menagkap hasil lalu lintas jaringan komputer dalam bentuk capture record dengan berbagai kondisi dan jenis alamat IP Address. Aplikasiini dapat bekerja secara real time atau up to date melalui server sekarang dalam menangkap paket-paketdata atau informasi dalam berbagai format protokol sehingga tools mampu dengan mudah menampilkan hasilnya dalam interface yang mudah dipahami olehuser Wireshark.

2. Landasan Teori

Aktivitas Ilegal

Kegiatan ilegal merupakan kegiatan yang melanggar peraturan, etika dan norma bagi pelakukegiatan ilegal tersebut. Contoh dari kegiatan terseut ialah menggunakan jaringan komputer untuk mengakses sebuah sistem yang bersifat privat. Komputer yang terhubung ke network, mempunyai ancaman kemanan lebih besar dari pada komputer yang berdiri sendiri (standalone). Dengan pengendalian yang teliti, resiko tersebutdapat dikurangi. Namun network security biasanya bertentangan dengan network a ccess semakin mudah,maka network security semakin rawan dan bila network security semakin baik, network access semakin tidak nyaman. Suatu network didesain sebagai komunikasi data highway dengan tujuan meningkatkan akses kesistem komputer, sementara security didesain untuk mengontrol akses. Penyediaannetwork security adalah sebagai aksi penyeimbangatara open access dengan security[1].

Salah satu aksi pelaku kegiatan ilegal untuk mencapai tujuan dipastikan telah memenuhi persaratanberupa informasi data yang valid. Teknologi digital signature atau tanda digital dapat digunakan sebagai intellectual property dengan menandai informasi tetrsebut pelaku dapat melakukan kegiatan ilegal dengan lancar. Adapun

kasus lain yang mendapatkan accsess control, berkaitan dengan pembatasan hak akses orang yang dapat mengakses informasi.

Cara standar yang digunakan untuk access control yaitudengan login dan password[1].

Kasus terakhir yaitu berupa ketesediaan informasi. Contohnya melakukan tracking atau pelacakan server yang didapatkan dengan permintaan palsu secara berkala sehingga tidak dapat melayani permintaan yang lain. Kasus ini mengakibatkan sejumlah informasi tidak bisa diakses secara normal.

Penyalahgunaan Protocol TCP

TCP (Transmision Control Protocol) adalah sebuah protokol yang menyediakan layananpengiriman data, TCP merupakan protokol yang bersifat connection-oriented, reliable, byte stream service.

Koneksi antara 2 aplikasi pengguna TCP harus memiliki izin akses untuk mempermudah dalammendapatkan informasi, sering terjadi pertukaraninformasi asli dengan informasi buatan pelaku kegiatan ilegal sehingga data asli dimiliki pelaku. Sebelum melakukan akses data akan dilakukan deteksikesalahan paket TCP dan merubah kembali data informasi yang telah diketahui. Data yang asli dapat digunakan untuk mengakses secara terus menerus tanpa ada batasan jika data informasi tersebut tidak dilakukan recovery data dan mengubah hak akses ataulebih mudahnya merubah domain dari data tersebut.

Permintaan Data Palsu

Pengiriman data secara terus menerus menimbulkan adanya perubahan pada sistem untuk menseleksi informasi. Informasi akan sulit di akses maupun tidak bisa diakses hal ini dikarenakan adanya penumpukan perintah untuk mengakses secara terus menerus sehingga pada saat carture akan menduplikatinformasi.

Kesulitan dalam mengakses informasi yang ada akan memberatkan data dan penerima data, hal ini sangat mengganggu ketika digunakan oleh pemmilik data. Pelaku aktivitas ilegal akan mengirim data yang seharusnya tidak perlu digunakan oleh pemilik data, namun data yan dikirim akan dikirim untuk merusak jaringan data yang digunakan pemilik data. Data yang telah digunakan korban (pemilik data informasi) akan mengakibatkan lambatnya jalur jaringan atau bisa merusak perangkat keras apabila jenis data yang dikirim pelaku mengandung virus untuk mempengaruhi sistem pada perangkat keras korban. Apabila hal ini dilakukan secara terus menerus akan memungkinkan pelaku untuk mengakses data informasi dan memanipulasi data yang telah didapatkankan pelaku. Pelaku dapat melihatseluruhaktifitas data informasi tersebut ketika digunakan.

3. Metode Penelitian

Wireshark

Wireshark banyak digunakan dalam memecahkan troubleshooting dijaringan untuk memeriksa. keamanan jaringan, men-debug implementasi protocoljaringan dalam software mereka, melakukan debugging implementasi paket protocol, serta belajar. protocol dan banyak juga digunakan untuk sniffer ataumengendus data-data privasi dijaringan. Wireshark inidiibaratkan sebagai media atau tool yang dapat dipakaioleh user untuk penggunaanya, apakah untuk kebaikanatau kejahatan. melalui antarmuka yang telah ditentukan dan selanjutnya menampilkannya. Jika Komputer terhubung dengan jaringan kecepatan tinggidan pada computer sedang digunakan aplikasi berbasis jaringan, aplikasi wireshark akan menampilakan banyak sekali paket data dan menimbulkan kebingungan karena ada begitu banyak paket data jaringan yang muncul. Aplikasi wireshark dapat memfilter jenis protocol tertentu yang ingin ditampilkan[1].

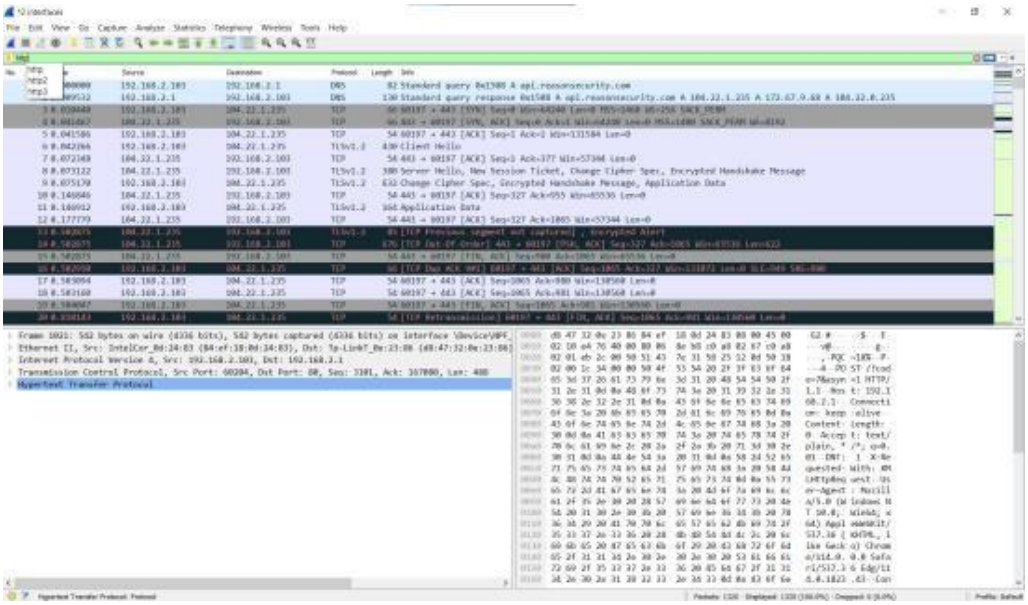
Hal ini karena wireshark dapat digunakan untuk mencari informasi yang sensitif yang berkeliaran padajaringan, contoh nya kata sandi, cookie dan lain sebagainnya. Wireshark dapat menganalisis paket datasecara real time. Artinya aplikasi wireshark ini akan mengawasi semua paket data yang keluar masuk melalui antar muka yang telah di tentukan oleh user sebelumnya. Wireshark dapat menganalisa paket data secara real time artinya, aplikasi wireshark akan mengawasi semua paket data yang keluar masuk.

Analisa Hasil Capture Aktivitas Ilegal

Analisa yang digunakan dalam kasus ini ialahanalisa TCP pada scanning sistem jaringan. Penellitianpada kasus ini dilakukan dengan pendekatan pengembangan, dengan metode ini pemilik data bisa melihat data yang dimiikinya aman untuk digunakan atau tidak aman ketika digunakan. Untuk mengantisipasi adanya kebocoran data informasi dan meminimalisir adanya hilangnya data.

Rancannngan Sistem Jaringan Aktivitas Ilegal

Rancangan pada bagian ini menggunakan software Wireshark seagai alat capture yang bergerakpada sistem operasi windows 10 bisa kita lihat pada gambar berikut ini.



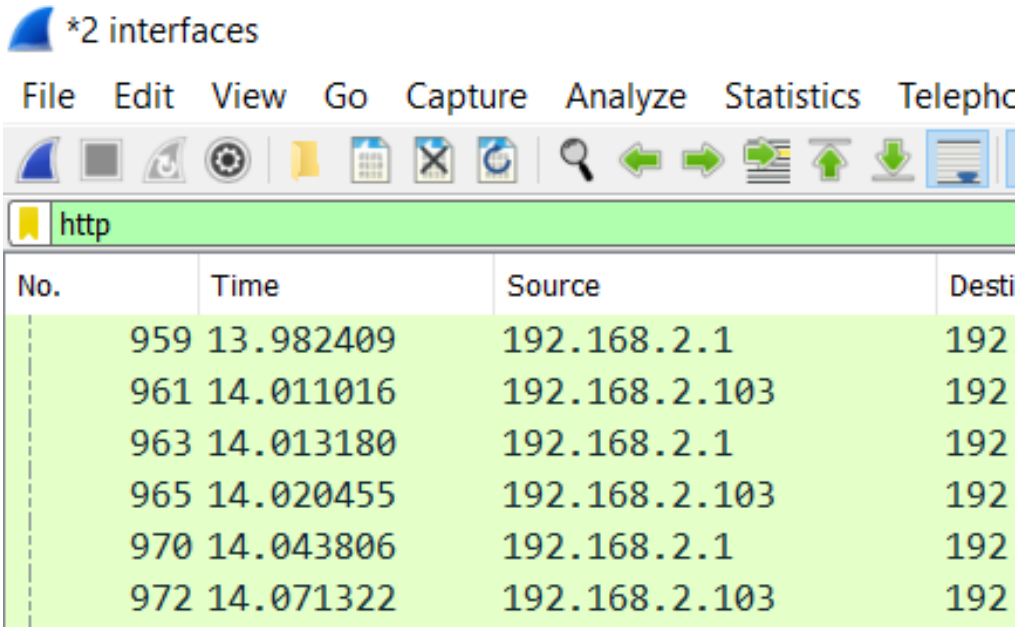
Gambar1. Wireshark

4. Hasil Penelitian

Pada hasil capture terlihat jika semua aktivitas jaringan yang melalui lalu lintas jaringan akan tercapture dengan detail dari TCP sampai waktu ketikamengakses alamat atau IP Address.

Filter Hasil Capture Jaringan

Pada kolom sharch pengguna bisa melakukan beberapaperintah untuk mengakses format atau akses apa yang ingin dilakukan, pada kasus ini pengguna memasukkan perintah untuk mengakses HTTP sehingga pada kolomHTTP akan terfilter seara otomatis dan bisa diproses lebih lanjut jika diperlukan.



Gambar 2. Filter Hasil Capture

5. Kesimpulan

Setelah melakukan proses capture kita bisa mengetahui dari cara kerja tools Wireshark dalam menyediakan paket dalam melakkukan capture data namun dalam kasus ini hanya dijelaskan bagaimana cara mengcapture aktivitas ilegal pada lalu lintas jarigan.

Dari hasil capture tadi bisa kita simpan sebagai bahan oleh data untuk melakukan kegiatan forensik digital jika diperlukan, data yang tersimpan menjadi bukti kuat dalam sebuah proses penegakan hukumkasus digital

6. Daftar Pustaka

[1] D. T, “ANALISA PENCEGAHAN AKTIVITAS ILEGAL DIDALAM JARINGAN MENGGUNAKAN WIRESHARK, 2015.
[2] Susianto, “IMPLEMENTASI DAN ANALISIS JARINGAN MENGGUNAKAN WIRESHARK, CAIN AND ABELS, NETWORK MINNER (Studi Kasus: AMIK Dian Cipta Cendikia),” 2018.
[3] A. K. W. M. Wireshark, “Tri Novita R,” 2021.