Analisis Layer Aplikasi (Protokol *HTTP*) menggunakan Wireshark

Muslimah Katoningati [a*], Indra Gunawan [b*], Raniah Inas Salsabila [c], Anggita Eka Dewi Melania[d]

[abcd c]Teknik informatika;Sekolah Tinggi Teknologi Ronggolawe Cepu;

[b] Penulis Korenspondensi, Alamat Email: igunsttr@gmail.com

Abstract

The Open Systems Interconnection Model or OSI Model is a structured logic framework that regulates the data communication process on the network. which it uses to exchange information. In the exchange of information between applications running on the sending host and the destination host, various application layer protocols are used to determine how messages are exchanged between the sending and destination hosts, the syntax of the data format control commands being exchanged, the methods used to detect errors and how to resolve errors. that, as well as how the interaction with the layer below it. There are many protocols for the application layer, including (control command, Domain Name Service Protocol (DNS), Hypertext Transfer Protocol (HTTP)

Keywords *— Wireshark, HTTP, security analysis.*

Abstrak

Open Systems Interconnection Model atau OSI Model merupakan kerangka logika terstruktur yang mengatur proses komunikasi data pada jaringan. yang digunakannya untuk melakukan pertukaran informasi. Pada pertukaran informasi antar aplikasi yang berjalan pada host pengirim dan host tujuan digunakan berbagai protokol Application Layer menentukan bagaimana pesan dipertukarkan antara host pengirim dan tujuan, sintaks dari perintah-perintah control format data yang dipertukarkan, metode yang digunakan untuk mengetahui terjadinya kesalahan dan bagaimana mengatasi kesalahan tersebut, serta bagaimana interaksi dengan layer yang berada di bawahnya. Terdapat banyak protokol untuk apllication layer, antara lain (control command Domain Name Service Protocol (DNS), Hypertext Transfer Protocol (HTTP)

.

Kata Kunci *—wireshark, HTTP, analisis keamanan*

1. Pendahuluan

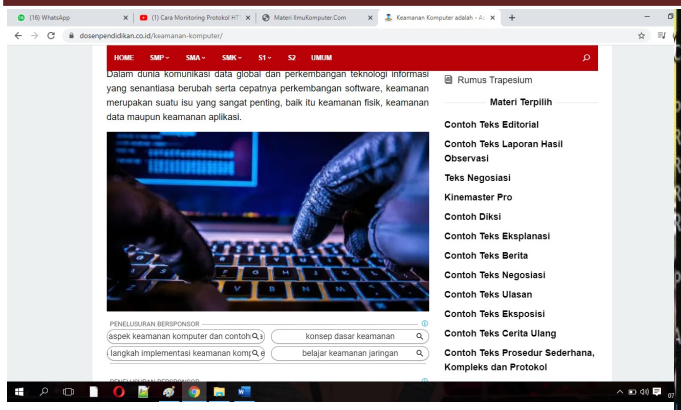
Application Layer merupakan layer paling atas, baik pada model OSI, maupun model TCP/IP. Layer ini menyediakan antarmuka antara aplikasi-aplikasi yang kita gunakan, dengan jaringan yang digunakannya untuk melakukan pertukaran informasi. Pada pertukaran informasi antar aplikasi yang berjalan pada host pengirim dan host tujuan digunakan berbagai protokol Application Layer.

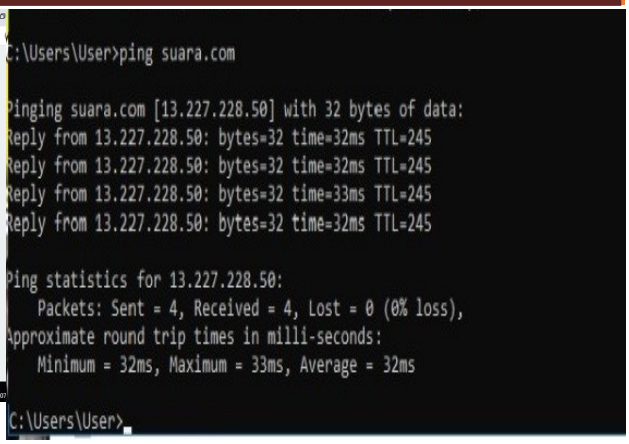
Protokol pada application layer menentukan bagaimana pesan dipertukarkan antara host pengirim dan tujuan, sintaks dari perintah-perintah kontrol (control command), jenis dan format data yang dipertukarkan, metode yang digunakan untuk mengetahui terjadinya kesalahan dan bagaimana mengatasi kesalahan tersebut, serta bagaimana interaksi dengan layer yang berada di bawahnya. Terdapat banyak protokol untuk apllication layer, antara lain Domain Name Service Protocol (DNS), Hypertext Transfer Protocol (HTTP)

2. Cara Menjalankan Wireshark: Meng-capture paket data pada protokol HTTP

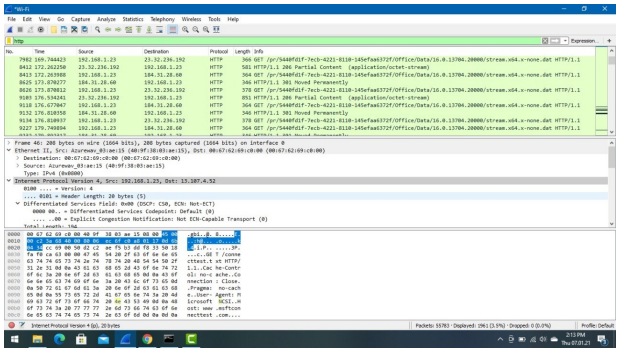
Hypertext Transfer Protocol (HTTP), pada awalnya merupakan prokol yang dikembangkan untuk mempublikasikan maupun mengunduh halaman HTML. Saat ini, HTTP yang merupakan protokol pada application layer yang paling sering digunakan juga dimanfaatkan untuk transfer data. HTTP menentukan mendefinisikan protokol dalam melakukan request dan response antar klien dan server. Dengan HTTP, terdapat tiga jenis pesan yang dipertukarkan, yaitu GET, POST, dan PUT. GET digunakan oleh klien untuk melakukan request. POST dan PUT digunakan untuk melakukan upload data ke server. Dan berikut tampilan cara meng-capture paket data melalui Wireshark yang dikirimkan saat sedang membuka web browser, sehingga paket melewati protokol HTTP:

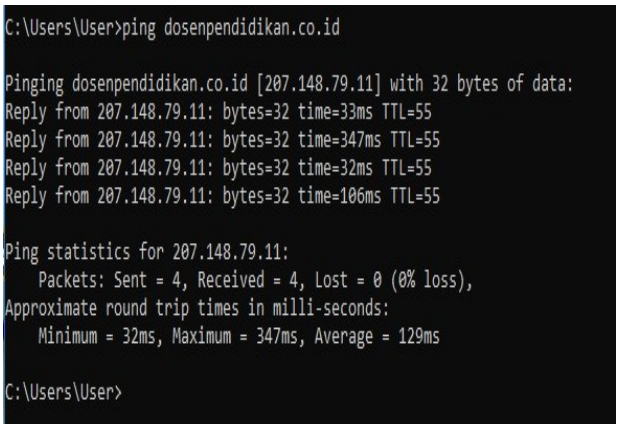
2.1. Setelah itu, buka web browser (contoh Mozilla Firefox) kemudian buka situs apapun (contoh suara com ,dosenpendidikan co.id)



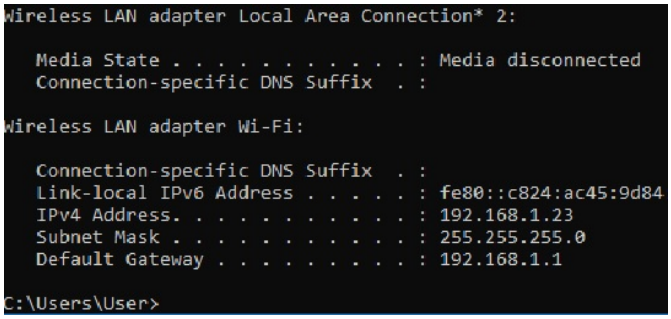


2.2. Saat situs-situs diakses dan terbuka, maka saat itu pula data-data telah dimasuk ke Wireshark dan paket-paket data pun akan ditampilkan.





2.3. Kemudian, melakukan pengecekan IP Address laptop kita (untuk keperluan pembuktian), dengan cara : klik Start>mengetik cmd pada kotak Search> OK. Setelah muncul kotak dialog Command Prompt, mengetikkan 'ipconfig' dan terbacalah bahwa IP Address Laptop kita yaitu 192.168.1.23

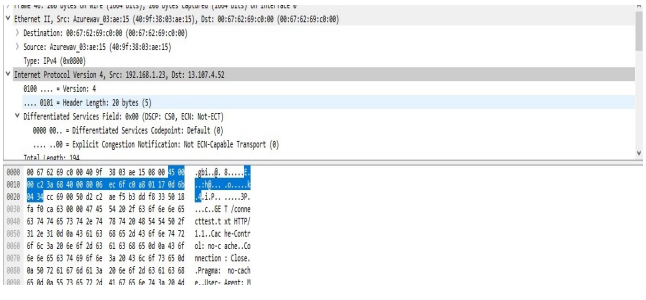


2.4. Setelah itu melakukan pengecekan IP Address dari situs yang kita buka melalui Command Prompt, antara lain: suara.com (IP Address:13.227.228.50); dosenpendidikan co.id (IP Address:207.148.79.11).

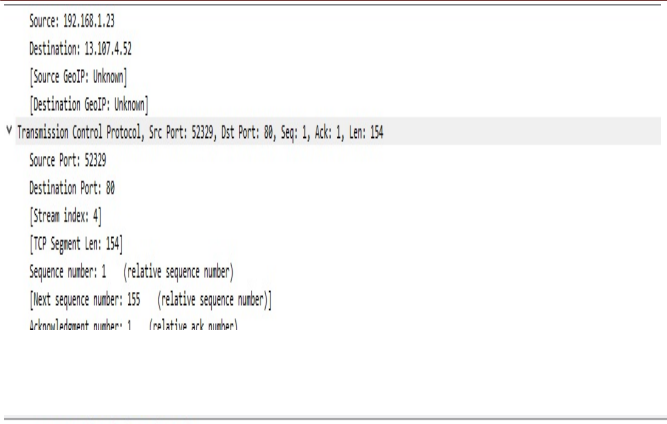
3. Hasil dan Pembahasan

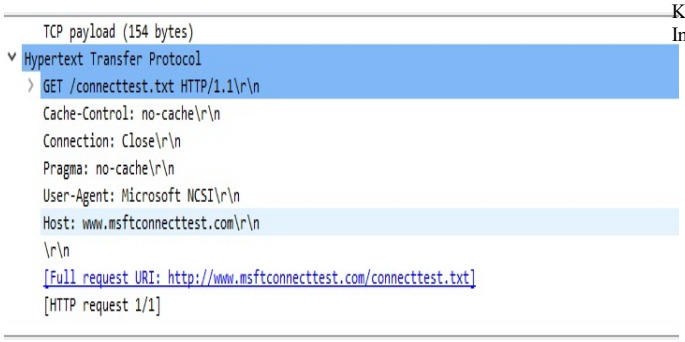
Kita telah mengakses situs melalui web browser dan telah menampilkan lalu lintas paket data nya melalui Wireshark. Disini ada ETHERNET, TCP dan HTTP dari browser yang dicari dosenpendidikan co.id belajar keamanan infromasi dan jaringan seperti berikut:

Dari hasil Ethernet II Dst (00:67:62:69:c0:00), Destination (00:67:62:69:c0:00), Source (40:9f:38:03:ae:15)



Dari hasil TCP port sumbernya 52329 , port tujuan(HTTP) 80, Seq 1, Ack 1, Len 154





4. Kesimpulan

Metode yang digunakan pada protokol HTTP adalah GET, metode GET meminta representasi dari sumber server yang dituju untuk meminta halaman sumber tertentu.

Daftar Pustaka

Cahyanintyas, Amelia. (2007). Monitoring Layer Aplikasi (Protokol HTTP)
Data Jaringan Menggunakan Wireshark. Yogyakarta: Andi. 2011

Gunawan; Indra, Ferriyan; Andrey. (2016). Analisis Keamanan Jaringan Wifi

Gunawan; Indra.(2021). *Keamanan Data: Teori dan Implementasi*. Jejak Publisher: Sukabumi. Diunduh dari https://www.researchgate.net/publication/338598999_Keamanan_Data_Teori_dan_Implementasi

Gunawan; Indra, Ferriyan; Andrey. (2016). Analisis Keamanan Jaringan Wifi
Informasi & Teknologi Informasi (SENSITIF). Diunduh dari https://www.researchgate.net/publication/316464159_Analisis_Keamanan_Jaringan_Wifi_Pendekatan_Blackbox_dan_Whitebox_Studi_Kasus_Ibnu_Sina_Batam

Kurniawan A, (2013). Network Forensics: Panduan Analisis Dan Investigasi Paket
Menggunakan Wireshark. Ilmu Komputer.Com. https://ilmukomputer.org/2013/06/02/monitoring-layer-aplikasi-protokol http-menggunakan-wireshark/
Pendekatan Blackbox dan Whitebox. *Seminar Nasional Sistem*