**Analisis Trafik**

**Disusun Oleh:**

Muhammad Ikhwan Perwira

09011282025077

**Fakultas:**

Ilmu Komputer

**Jurusan:**

Sistem Komputer (3A)

**Mata Kuliah:**

**Komunikasi Data**

**Dosen Pengampu:**

Adi Hermansyah, M. T.

**Universitas Sriwijaya**

**Tahun Ajaran 2020/2021**

**DAFTAR ISI**

* Cover
* Daftar Isi
* Abstrak
* Kata Pengantar
* Pendahuluan
* Latar Belakang
* Rumusan Masalah
* Tujuan Pembahasan
* Isi
* Kesimpulan
* Saran
* Penutup
* Daftar Pustaka

**ABSTRAK**

Dalam laporan ini berisi mengenai definisi-definisi pada Layer OSI, perbedaan UDP dan TCP, Protokol Data Unit, TCP Header, TCP 3 Ways Handsake, Encrypted Packet vs Non-Encrypted Packet. Selain pejelasan diatas juga akan dijelaskan pokok analisa trafik yaitu mencari parameter QoS (Quality of Service).

Parameter Quality of Service seperti *throughput, latency, jitter, packet loss*. Perbedaan *throughput* dengan *bandwidth*. Perbedaan *latency, delay* dengan *ping*. Perbedaan *jitter* dan *delay*. Menganalisa *packet loss* pada wireshark.

Adapun objek yang penulis analisa adalah Video Streaming di situs web *ikhwanperwira.my.id* dan situs web pada *example.com*.

**PENDAHULUAN**

Wireshark adalah sebuah aplikasi capture paket data berbasis open-source yang berguna untuk memindai dan menangkap trafik data pada jaringan internet. Aplikasi ini umum digunakan sebagai alat troubleshoot pada jaringan yang bermasalah, selain itu juga biasa digunakan untuk pengujian software karena kemampuannya untuk membaca konten dari tiap paket trafik data. Aplikasi ini sebelumnya dikenal dengan nama Ethereal, namun karena permasalahan merek dagang lalu namanya diubah menjadi Wireshark. Wireshark dapat digunakan untuk menganalisa Quality of Service yang meliputi parameter, delay, jitter, througput, latency, packet loss.

Quality of Service (QoS) atau Kualitas layanan adalah metode pengukuran yang digunakan untuk menentukan kemampuan sebuah jaringan seperti; aplikasi jaringan, host atau router dengan tujuan memberikan network service yang lebih baik dan terencana sehingga dapat memenuhi kebutuhan suatu layanan.

Parameter kualitas yang dinilai meliputi throughput, latency, jitter, packet loss.

Tahap untuk melakukan penilaian QoS adalah Capturing, Filtering, Analysis.

**LATAR BELAKANG**

Streaming adalah proses pengiriman data tanpa harus mengunduh keseluruhan data terlebih dahulu melalui *buffering* begitupun juga dengan pengunggahan data. Streaming sering dipakai dalam video streaming. Dalam kasus ini penulis memilih untuk menganalisa proses streaming dalam suatu video di server penulis untuk menganalisa Quality of Service.

Transport Layer Security (TLS) adalah protokol yang menangani kriptografi untuk memberikan keamanan komunikasi melalui jaringan komputer. TLS adalah penerus dari SSL (Secure Socket Layer). TLS bertujuan agar trafik komunikasi lebih susah untuk di-*sniffing. Sniffing* adalah tindakan penyadapan yang dilakukan melalui sebuah jaringan. Wireshark sendiri bisa digunakan sebagai alat penyadap, namun karena TLS mengenkripsi data-data yang dikirim, maka data yang tertampil berupa *cipher text* bukannya *plain text*. *Cipher text* adalah teks tersandi yaitu teks yang dihasilkan dari proses enkripsi sehingga pada umumnya *cipher text* terlihat seperti teks yang bersifat acak dan tidak dapat dimaknai oleh manusia. Sedangkan *plain text* adalah teks terang yaitu teks normal pada umumnya yang dapat dimaknai dan dimengerti oleh manusia.

**RUMUSAN MASALAH**

1. Mahasiswa dapat mencari nilai thoroughput menggunakan wireshark
2. Mahasiswa dapat mencari nilai latency menggunakan wireshark.
3. Mahasiswa dapat mencari nilai jitter menggunakan wireshark.
4. Mahasiswa dapat mencari packet loss menggunakan wireshark.

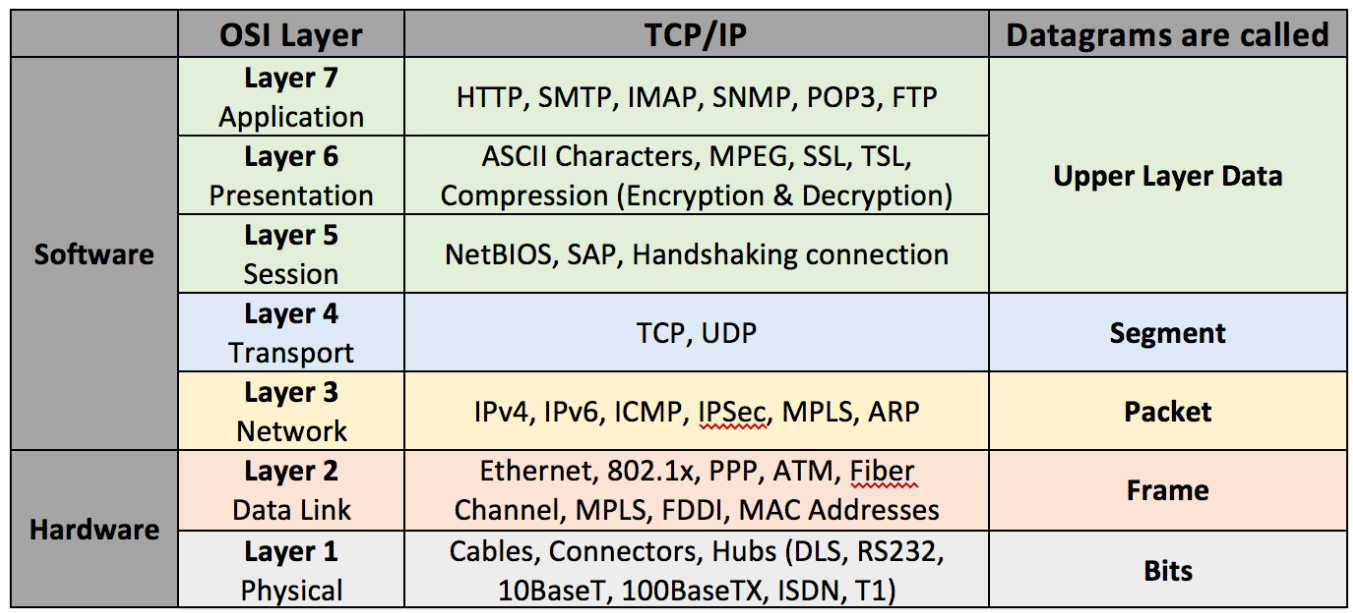
**TUJUAN PEMBAHASAN**

Adapun tujuan pembahasan diharapkan agar penulis dan pembaca dapat mengetahui model layer OSI, perbedaan UDP dan TCP, memahami Protokol Data Unit (PDU) dan hubungannya dengan layer OSI serta menerapkannya pada wireshark, memahami TCP Header, memahami establishing pada TCP serta perbedaan Encrypted Packet dengan Non-Encrypted Packet.

Selain itu agar penulis dan pembaca dapat mencari parameter Quality of Service menggunakan wireshark, serta membedakan antara bandwidth dengan throughput, membedakan ping, delay, dengan latency, serta dapat membedakan delay dengan jitter.

**Layer OSI**

Layer OSI (Open System Interconnection) adalah suatu model abstraksi jaringan yang sesuai dengan Standar Internasional dari ISO yang menyediakan kerangka logika terstruktur bagaimana proses komunikasi data berinteraksi melalui jaringan. Dulu komunikasi data yang melibatkan komputer dari vendor berbeda. Masing-masing vendor menggunakan protokol dan format data yang berbeda yang mengakibatkan tidak adanya kompatibiltas pada masing-masing perangkat.

Secara umum layer OSI dibagi 7 lapisan:

1. Physical Layer

* Mendefinisikan Media Transmisi Jaringan
* Sinkronisasi Bit
* Arsitektur Jaringan seperti Ethernet
* Topologi jaringan dan pengabelan.
* Network Interface Card berinteraksi dengan Media Kabel atau Radio
* Network Interface Card, Repeater, Hub

1. Data-Link Layer

* Bit-bit data dikelompokkan menjadi frame
* Mengoreksi kesalahan
* Flow Control
* Media Acces Control atau pengalamatan perangkat keras (MAC Address)

1. Network Layer

* Mendefinisikan Alamat-alamat IP serta menyediakan fungsi routing

1. Transport Layer

* Memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali.
* Membuat komunikasi menjadi reliabel khususnya protokol TCP.
* TCP, UDP

1. Session Layer

* Mendefinisikan bagaimana koneksi dimulai, dijaga, dan diakhiri.
* NETBIOS

1. Presentation Layer

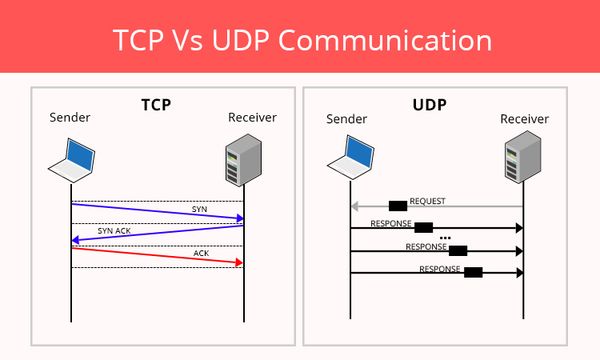
* RDP, VNC, SSH
* Mentranslasikan data yang hendak ditransmisi oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan.
* Mengenkripsi data yang hendak ditransmisikan (SSL, TLS).

1. Application Layer

* Sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan.
* Mengatur bagaimana aplikasi dapat mengakses jaringan.
* HTTP, FTP

**Perbedaan TCP dan UDP**

Baik TCP atau UDP pada model OSI berada di layer 4 yaitu Transport Layer. Yang membedakan antara keduanya adalah pada reliabilitasnya.

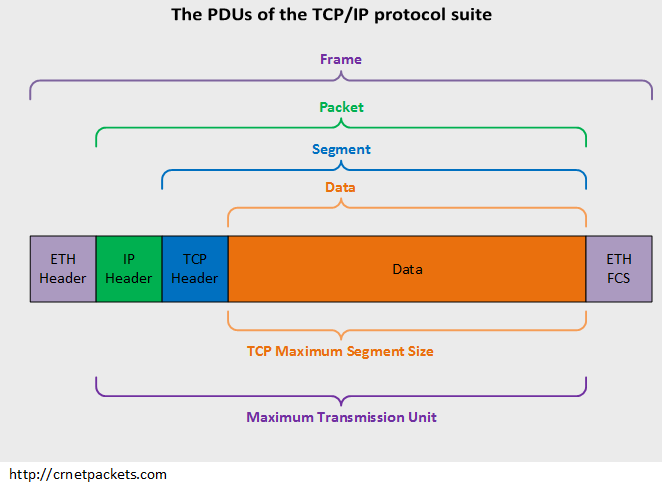
UDP lebih simple daripada TCP, oleh sebab itu Header pada UDP lebih sederhana daripada TCP.

Setiap proses transmisi data pada TCP yang dilakukan oleh pengirim, penerima wajib mengirim sinyal ACK (Acknowledgement) untuk memberitahu pengirim bahwa data yang diterima sudah berhasil dengan baik. Berbeda dengan UDP, pengirim data pada UDP tidak tau apakah data yang dikirimnya sudah diterima oleh penerima atau belum karena tidak adanya konfirmasi pengiriman data dari penerima seperti TCP yang menggunakan sinyal ACK. Begitupun juga dengan penerima yang tidak tahu apakah pengirim sudah mengirim data sebelumnya karena tidak adanya sinyal SYN (Syncronization).

Dari perbedaan diatas, dapat diketahui bahwa UDP lebih bersifat ke *broadcasting.* Sedangkan TCP memiliki kesepakatan untuk memulai koneksi terlebih dahulu *(establishing)* dengan menggunakan *3-ways handshake.*

**Protocol Data Unit**

Protocol Data Unit adalah pendefinisian satuan pada masing-masing protokol di dalam protokol.

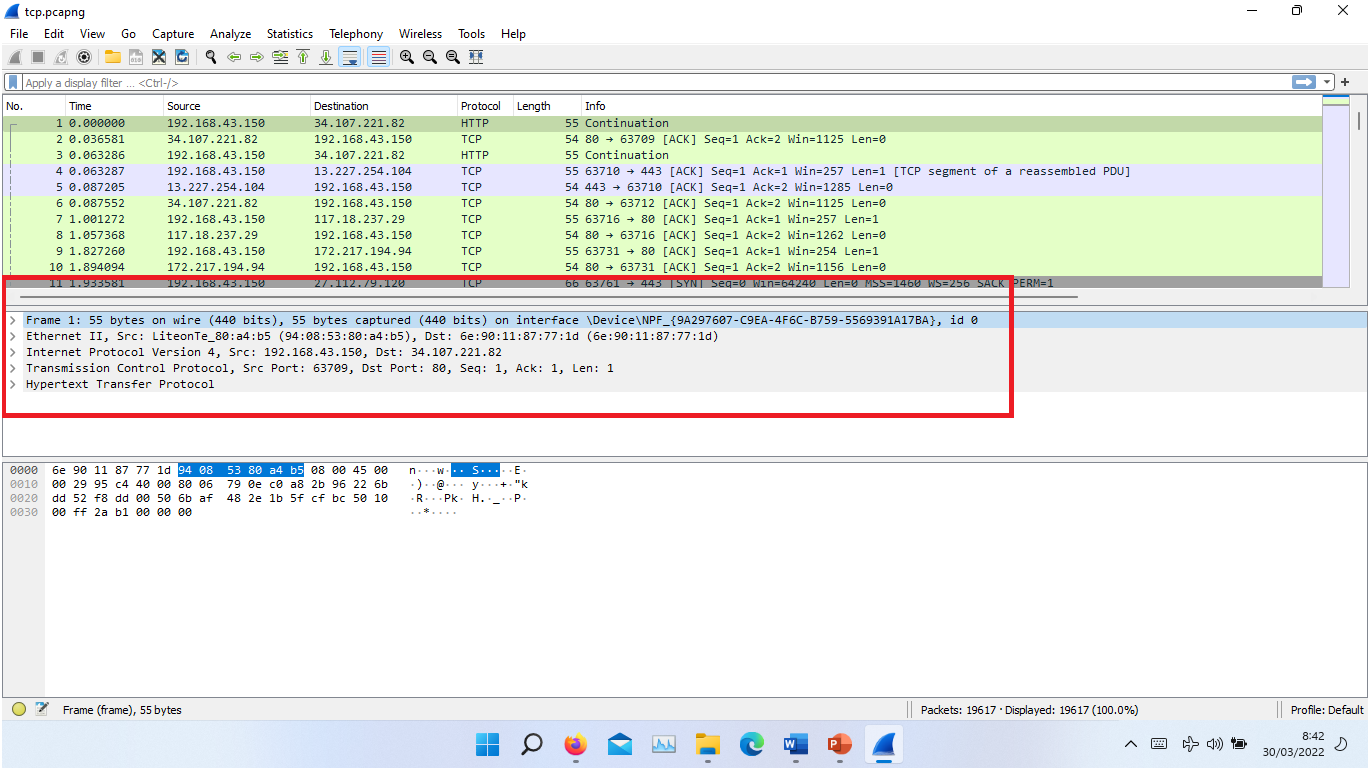
**

Jadi pada dasarnya tiap data dibungkus dari suatu protokol, dan protokol itu sendiri dibungkus dari protokol lainnya.

Pada umumnya data dari Ethernet Header sampai ke Ethernet Frame Check Sequence (ETH FCS) disebut dengan 1 Frame. Data yang dikandung Protokol Ethernet misalnya IP. Dari IP Header sampai ke Data disebut 1 Packet. Di dalam IP misalnya terdapat TCP, maka dari TCP header sampai ke Data disebut dengan 1 segment.

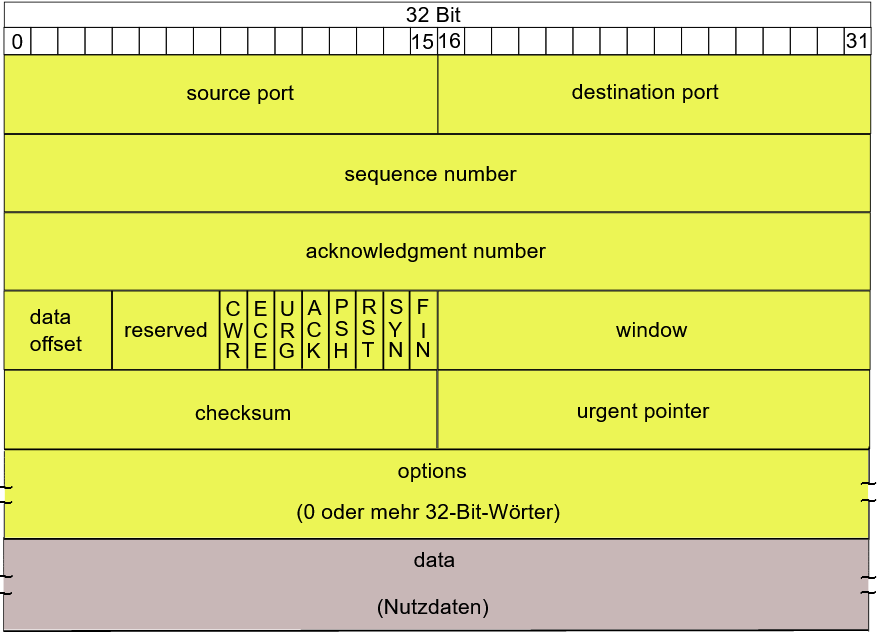
Maksimum byte-byte data yang dapat ditampung oleh ethernet disebut dengan Maximum Transmission Unit, biasanya berkisar sekitar 1500 byte. Sedangkan Maksimum byte-byte data yang dapat ditampung oleh TCP disebut dengan TCP Maximum Segment Size.

PDU terlihat dengan jelas ketika menganalisa dengan wireshark seperti pada gambar.



Protokol Data Unit jika kita perhatikan tidak lain dan tidak bukan adalah model layer pada OSI itu sendiri. Misalnya pada bagian ETH Header analogi dengan Data-Link Layer, IP Header analogi dengan Network Layer, TCP Header analogi dengan Transport Layer.

**TCP Header**

Setiap protokol memiliki header. Header pada protokol digunakan sebagai informasi awal untuk data yang hendak dikirim. Sehingga data yang dikirim memiliki kejelasan maksud dan tujuan pada data tersebut. Misalnya protokol TCP juga memiliki header pastinya. Format Header pada protokol TCP dapat dilihat pada gambar sebagai berikut. 

Pada gambar di atas, TCP Header cukup terlihat kompleks dibanding UDP Header. Penulis merangkum parameter apa saja yang terdapat pada TCP Header.

1. Source Port (16 bit)

Adalah port yang keluar pada pengirim.

1. Destination Port (16 bit)

Adalah port yang masuk pada penerima.

1. Sequence Number (32 bit)

Banyak byte data relatif yang telah dikirim sejauh ini.

1. Acknowledgement Number (32 bit)

Banyak byte data relatif yang telah diterima sejauh ini.

1. Data Offset (4 bit)

Adalah ukuran relatif atau banyaknya byte pada header.

1. Reserved (3 bit)

Adalah bit header yang akan digunakan atau belum diimplementasikan.

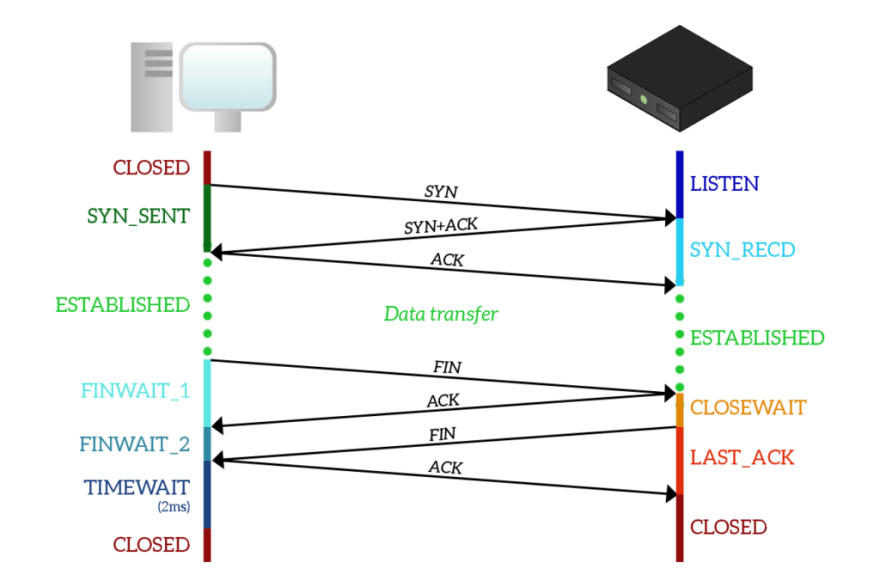
1. Flags bit (9 bit)

* URG: Urgent Flag digunakan untuk data yang bersifat mendesak.
* ACK: Acknowledgement Flag digunakan untuk mengakuisisi data yang telah diterima dengan mengirim sinyal ACK.
* PSH: Push Flag digunakan untuk mengirim data tanpa harus menunggu keseluruhan data tersebut. Push Flag mendorong data langsung ke application.
* RST: Reset Flag, mengakhiri koneksi dengan tidak normal.
* SYN: Syncronize Bit, yaitu bit yang digunakan untuk memulai koneksi (*establishing*) atau jabat tangan kedua perangkat.
* FIN: Finish Bit, untuk mengakhiri koneksi dengan normal.

1. Checksum (16 bit): adalah penjumlahan keseluruhan header yang digunakan untuk mendeteksi error atau data yang korup.

**TCP Life-Cycle**

Establishing pada TCP diperlukan untuk menjamin keandalan dalam komunikasi data pada protokol ini. Pada umumnya, life cycle pada TCP terdiri dari *establishing, transmitting, finishing.*

**

Pada tahap establishing juga disebut dengan jabat tangan 3-arah adalah proses memulai komunikasi antara dua perangkat. Pengirim mengirim sinyal *SYN* ke penerima untuk memberitahu penerima bahwa akan terjadinya komunikasi data, kemudian penerima mengirim sinyal SYN+ACK ke pengirim untuk memberi tahu penerima bahwa sinyal SYN yang dikirim tadi sudah diterima oleh penerima. Kemudian, pengirim mengirim sinyal ACK untuk memberitahu penerima bahwa sinyal SYN+ACK sudah diterima. Dari sini tahap establishing sudah dilakukan (established) yang kemudian dilanjutkan dengan tahap transmitting.

Pada tahap transmitting, pengirim mengirim data ke penerima. Selagi mengirim, penerima merespon balik tanggapan dari pengirim dengan mengirim sinyal ACK lebih tepatnya ACKNOWLEDGEMENT NUMBER untuk memberitahu pengirim bahwa berapa banyak data byte yang sudah diterima oleh penerima saat ini.

Ketika semua data sudah dikirim, pengirim atau penerima bisa mengakhiri koneksi dengan normal dengan mengirim sinyal FIN. Namun jika ada kendala, biasanya sinyal yang dikirim berupa sinyal RST. Misalkan penerima mengirim sinyal FIN duluan, maka kemudian pengirim merespon balik dengan mengirim sinyal ACK dan kemudian pengirim mengirim sinyal FIN ke penerima lalu penerima juga merespon balik dengan mengirim ACK. Maka koneksi sudah ditutup dengan lancar.

**Encrypted Packet vs Non-Encryped Packet**

Ketika paket tidak dienkripsi, maka data yang ditampilkan berupa data yang human readable sehingga menimbulkan resiko untuk mudah disadap dalam suatu jaringan. Dibandingkan dengan paket yang dienkripsi, ketika dilakukan penyadapan, data yang muncul di wireshark adalah data yang tidak bisa dibaca oleh manusia.

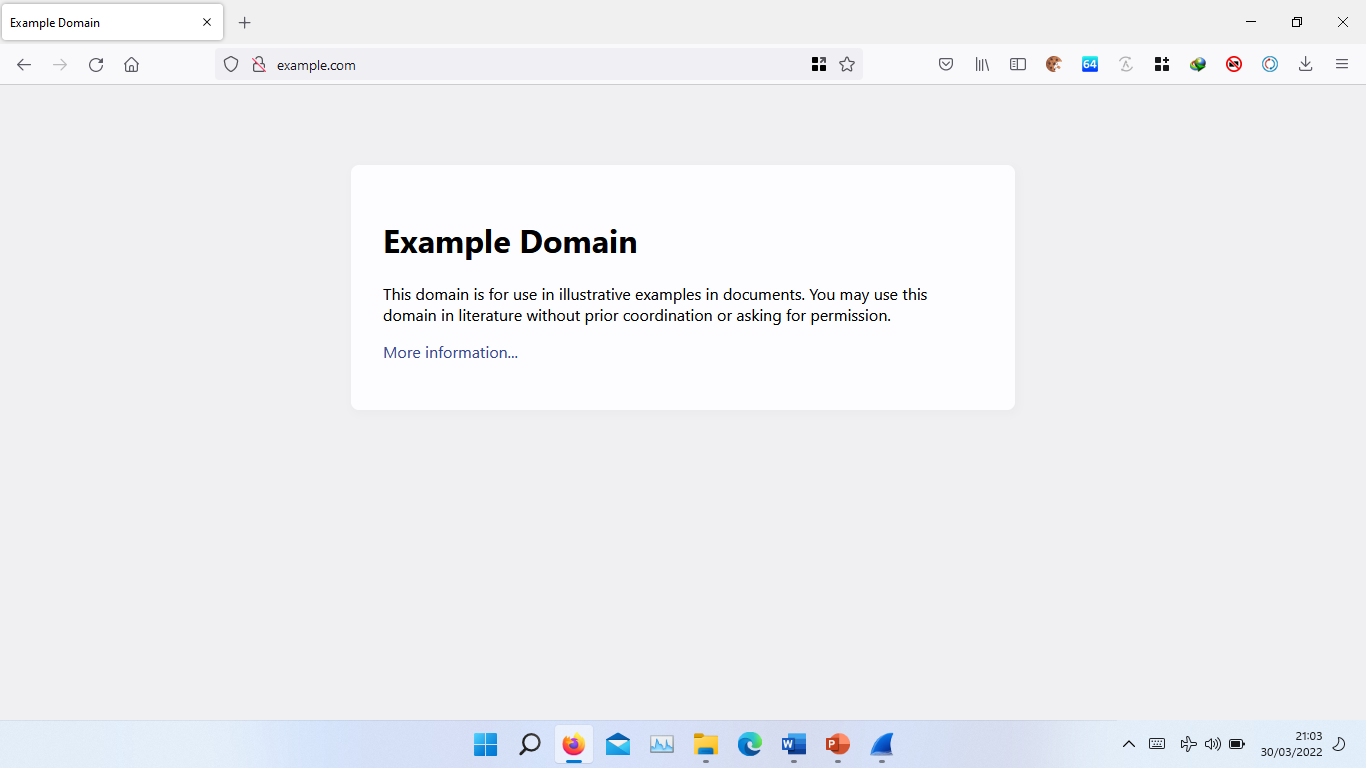
Sebagai contoh dalam analisa penulis dalam menganalisa web HTTP pada <http://example.com> dan HTTPS pada situs yang sama (<https://example.com>)

Terlihat sepele namun hal yang membedakan antara HTTP dan HTTPS adalah keamananya. HTTP merupakan kepanjangan dari *Hyper Text Transfer Protocol.* Sedangkan HTTPS merupakan kepanjangan dari *Hyper Text Transfer Protocol Secure.* Jadi yang membedakannya adalah keamanannya sadja.

Kita tahu bahwa HTTP adalah penerapan (aplikasi) dari TCP. Dan HTTPS merupakan penerapan dari TLS.

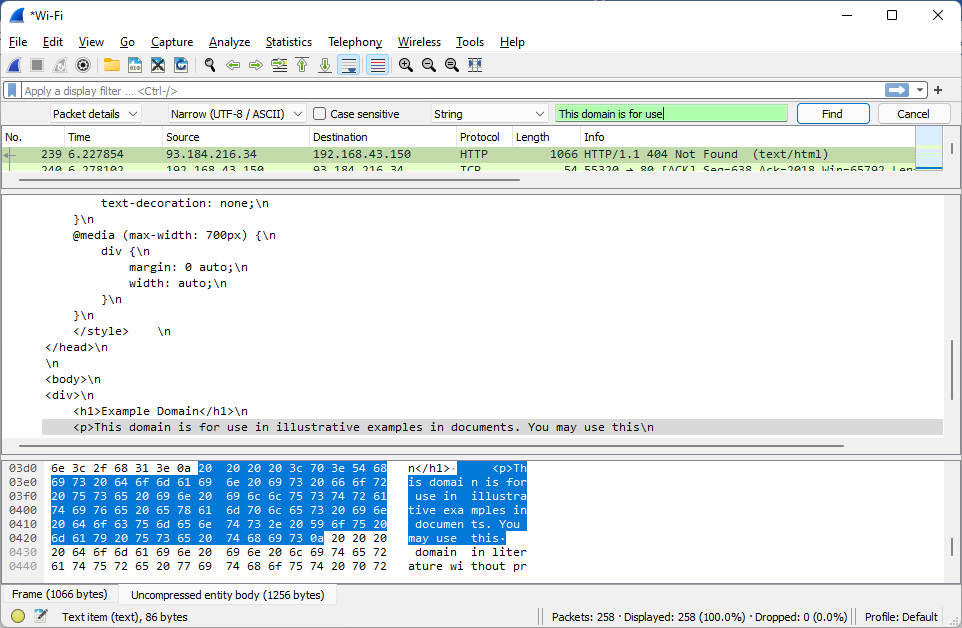
**Merekam** [**http://example.com**](http://example.com)

Pada kasus ini yang perlu dilakukan adalah menggunakan wireshark untuk menganalisa situs tersebut. Kemudian lakukan capturing, filtering, dan analyzing.



Terlihat pada URL Browser ada logo gembok yang dicoret menandakan bahwa koneksi tidak aman karena menggunakan protokol HTTP.

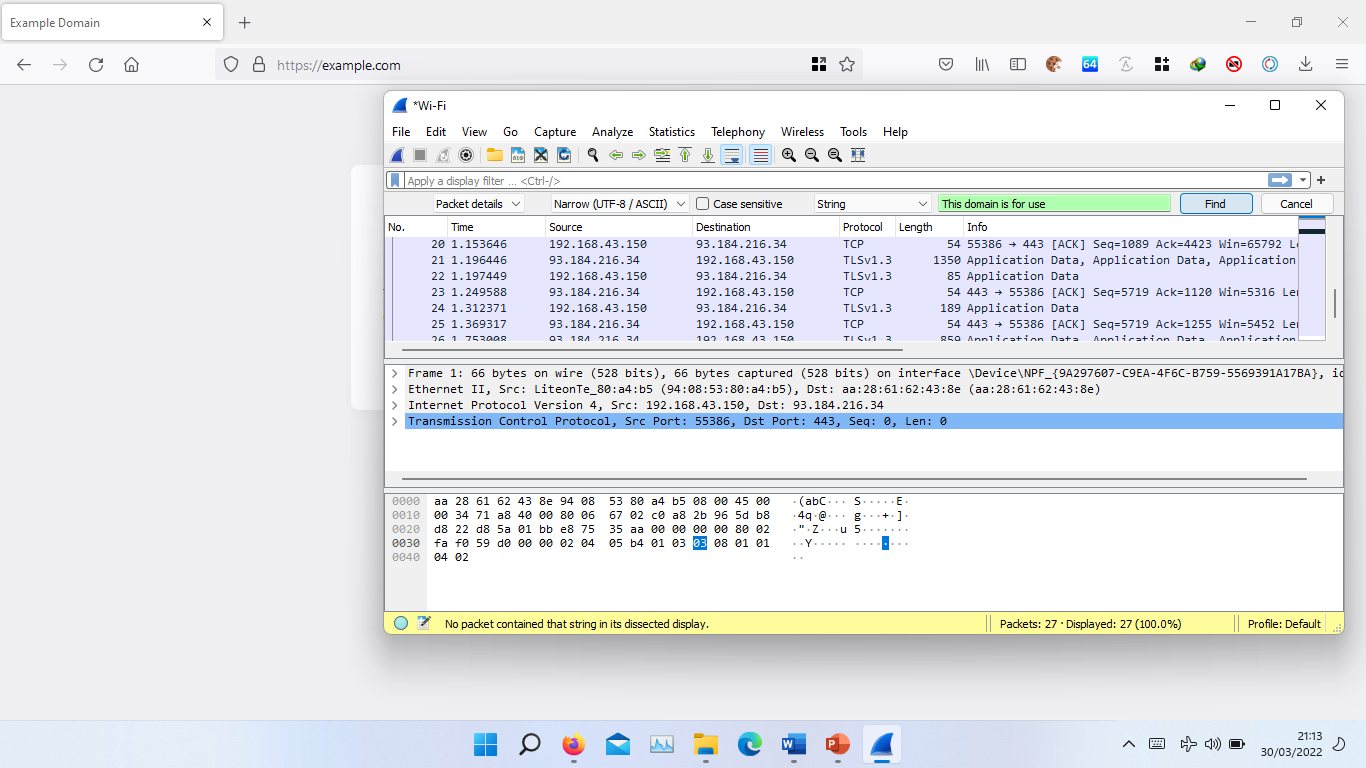
Karena situs tersebut tidak dienkripsi, maka data HTML tersebut dapat kita lihat melalui wireshark. Misalnya untuk mencari kata ‘**This Domain is for use**’sebagai sample, maka kita buktikan dengan menggunakan fitur *search* pada wireshark dengan menekan CTRL+F.



Terlihat bahwa kita bisa melihat isi data (html) pada situs tersebut karena paket tersebut tidak dienkripsi.

**Merekam** [**https://example.com**](https://example.com)

Sama seperti merekam <http://example.com>, disini yang perlu dilakukan adalah mengganti protokol yang digunakan dengan menambahkan huruf **s.**



Terlihat bahwa wireshark tidak dapat menemukan kata yang tertulis pada situs <https://example.com>.

Kesimpulan yang kita dapat adalah, menyadap data yang dienkripsi tetap bisa dilakukan, hanya saja kita perlu mencari kuncinya yang mana memerlukan skill Cyber Security.

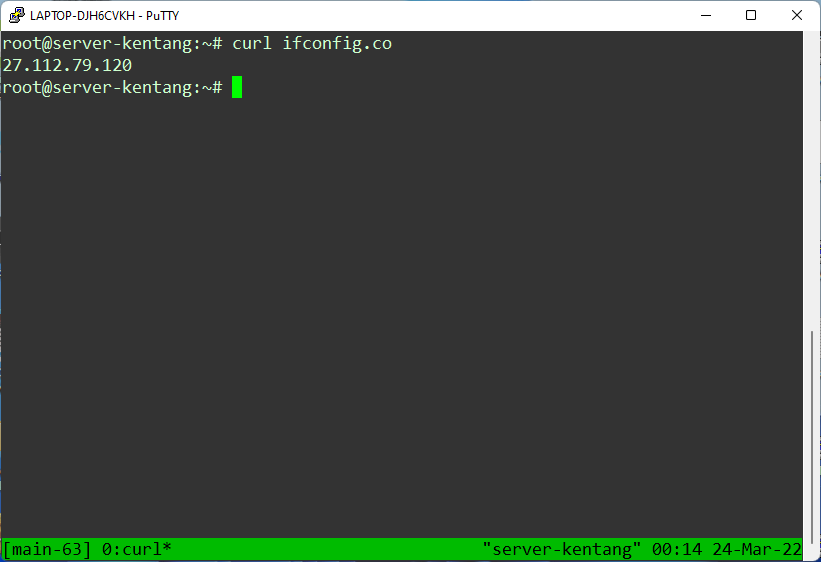
**Mencari Parameter Quality Of Service**

Seperti yang sudah dijelaskan sebelumnya bahwa parameter QoS terdiri dari *delay, latency, jitter, packetloss, throughput.*

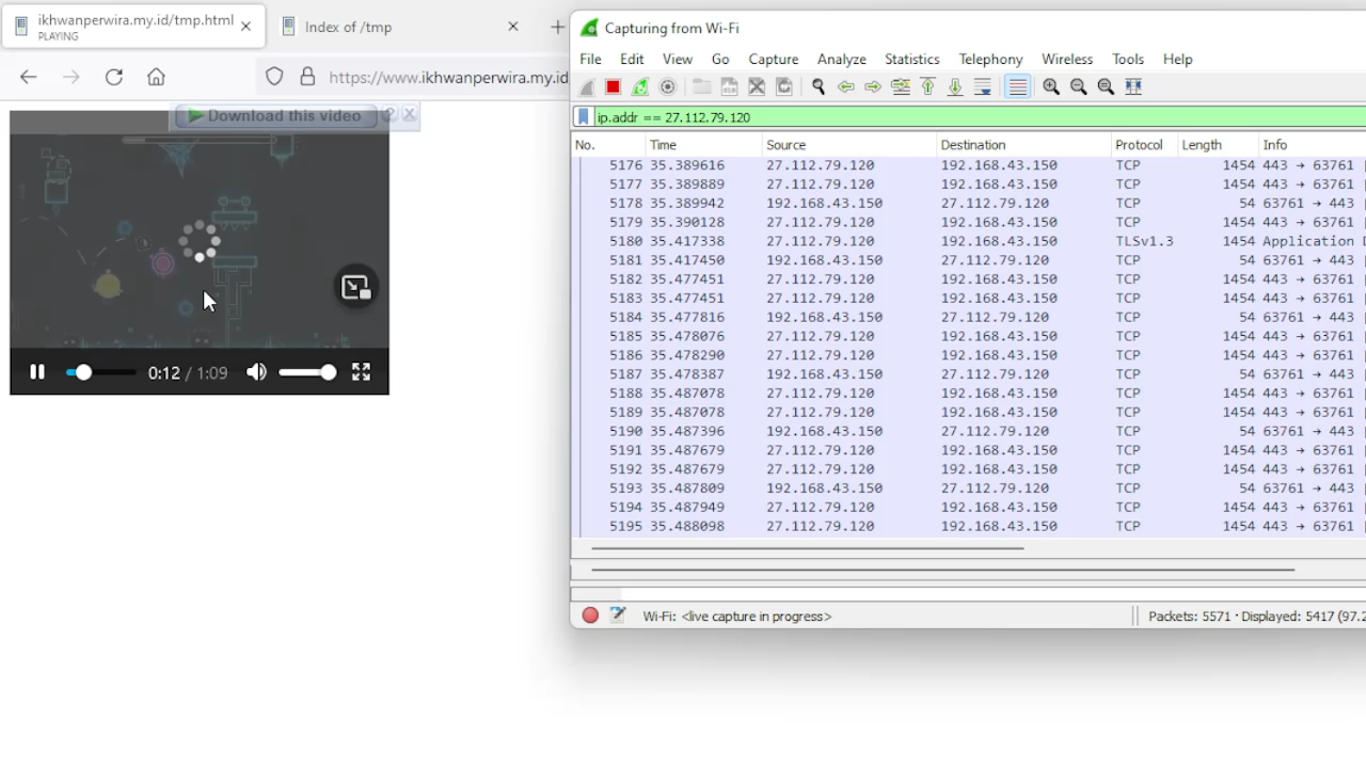
* Delay: adalah waktu tunda antara dua paket (memiliki satuan waktu atau second). Semakin besar nilai delay maka semakin lama paket tiba ke tujuan. Semakin kecil nilai delay maka semakin cepat paket tiba ke tujuan.
* Latency: adalah nilai rata-rata dari keseluruhan waktu tunda yang didapat (memiliki satuan waktu atau second). Semakin besar nilai delay maka semakin buruk karena rata-rata waktu yang diperlukan untuk mengirim atau menerima semakin lama dan sebaliknya jika nilai delay semakin kecil.
* Jitter: Rata-rata dari selisih dua waktu tunda mutlak. Dengan kata lain adalah variasi dari delay (memiliki satuan waktu atau second). Filosofi dari jitter adalah kestabilan dari waktu tunda. Semakin besar jitter maka fluktuasi waktu tunda semakin tinggi, oleh sebab itu kadang kita tanpa disadari jika pernah bilang (pingnya tidak stabil kadang naik kadang turun dengan cepat) ketika bermain game atau streaming yang sebenaranya nilai jitternya yang tinggi (konstan). Juga perlu dicatat bahwa ping dan latency adalah dua hal yang berbeda.
* Ping: PING adalah Packet Internet Gropher adalah suatu paket yang dikirim melalui protokol ICMP (memiliki satuan paket). Sering salah kaprah dengan latency padahal PING adalah paket yang dikirim bukan waktu paket yang dikirim.
* Throughput: adalah kecapatan byte-byte data yang diterima/dikirim (memiliki satuan byte/s).

**ISI**

Jadi pada kasus ini penulis menganalisa trafik streaming dari server penulis yang beralamat IP **27.112.79.120** sebagai source ke IP lokal penulis **192.168.43.150** sebagai IP Destination.



Adapun data yang dicapture adalah suatu video konten permainan bernama **Geometry Dash**. Ini adalah dokumentasi ketika dalam proses capturing.



Adapun file .pcap dan hasil analisanya ada di github

Jadi pada dasarnya untuk melakukan penilaian QoS ada tahapannya yaitu

**Capturing, Filtering, Analyzing.**

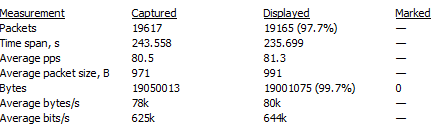
Pada tahap capturing, yaitu melakukan aksi komunikasi data di perangkat sehingga wireshark dapat merekam paket yang keluar ataupun masuk. Tahap Filtering yaitu menyaring paket-paket yang dibutuhkan saja, Tahap analyzing yaitu mencari parameter QoS.

Pada tahap filtering, saya harus menyaring IP Address server penulis yaitu **27.112.79.120** kemudian filter port juga yaitu **63761.**

Sehingga yang ditampilkan wireshark saat ini adalah komunikasi data yang penulis butuhkan.

Dalam kasus ini penulis mengekspor file csv dan konversi ke excel agar mudah dianalisa.

Adapun ringkasan statistik yang didapat dari wireshark adalah

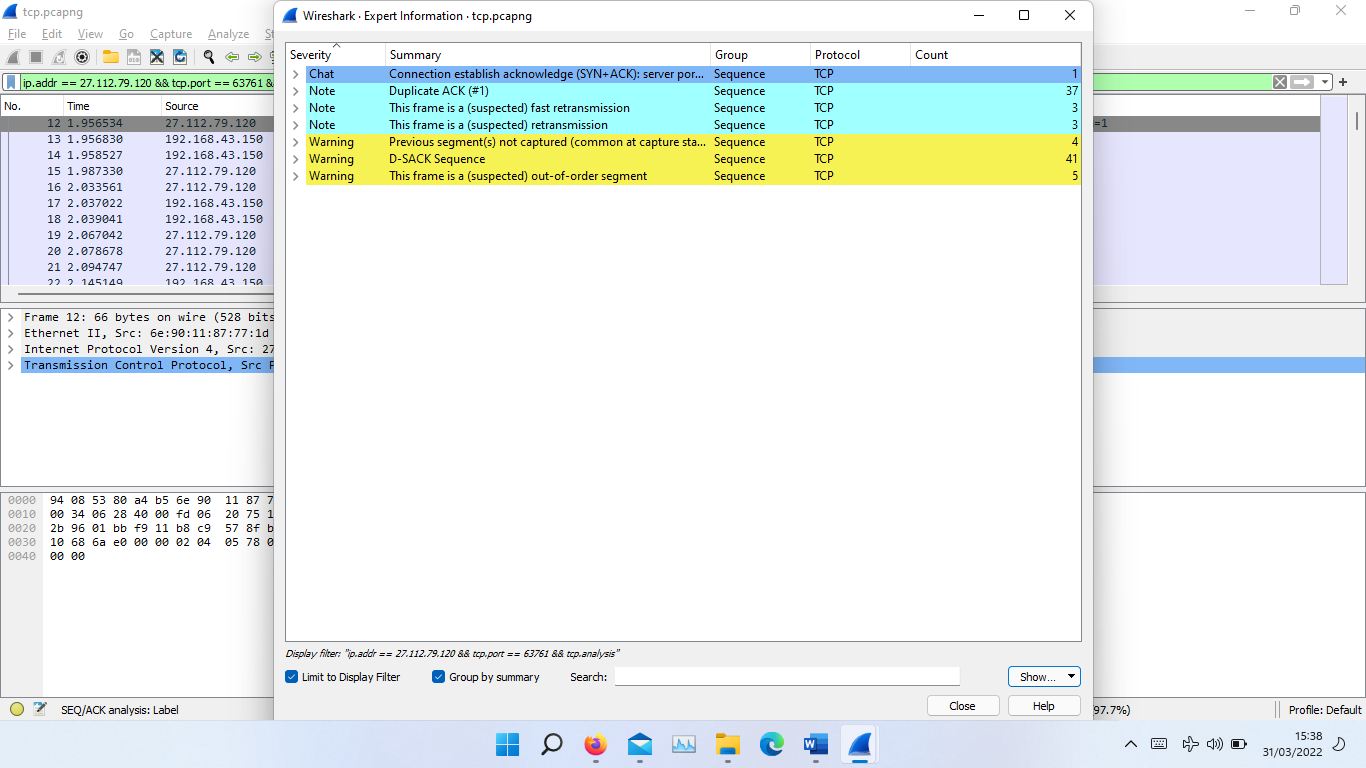


Kemudian untuk mencari latency adalah mencari delay terlebih dahulu, untuk mencari delay bisa didapat dengan membuat selisih antara waktu akhir kurang waktu awal. Waktu akhir kurang waktu awal dua paket disebut dengan delay. Lakukan sampai selisih waktu paket ke-19165 kurang paket ke-19164

Rata-rata dari keseluruhan delay disebut dengan latency

Untuk jitter, cari selisih dua delay. Kemudian dari kumpulan selisih tersebut mutlakan lalu cari rata-ratanya.

Untuk packet loss bisa filter dengan keyword **tcp.analysis.lost\_segment** atau bisa dilihat pada expert information



Terlihat ada beberapa note dan warning

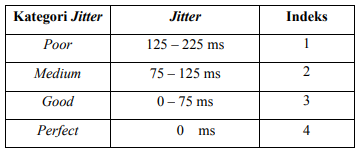
Untuk mencari persentase packetloss adalah banyak packetloss dibagi keseluruhan packet. Dalam kasus ini total warning dan total note yang terhitung adalah 37+3+3+4+41+5 dibagi dengan banyak seluruh paket (19165) adalah 0.48%

Adapun aplikasi rumusnya dapat dilihat pada file excel.

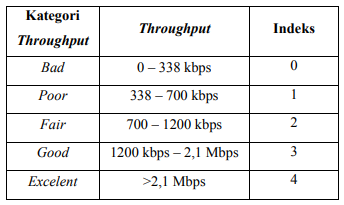
|  |  |
| --- | --- |
| Banyak Paket | 19165 |
| Time span (second) | 235.698928 |
| Average pps | 81.31135836 |
| Total Bytes | 19001075 |
| Total bit | 152008600 |
| Average packet size | 991.4466475 |
| Throughput(Bytes/s) | 80615.87365 |
| Throughput(bit/s) | 644926.9892 |
| Latency | 0.012299047 |
| Jitter | 0.020989661 |

**KESIMPULAN**

Semakin rendah jitter maka semakin baik (fluktuasi waktu tundanya rendah), dalam kasus ini nilai jitternya sebesar 20ms



Artinya jitternya adalah di rentang good.

Semakin tinggi nilai througput maka semakin baik karena semakin cepat komunikasi transfer dua data, dalam kasus ini nilai throughputnya adalah 80kb/s

Artinya throughput nya dalam keadaan buruk.

**SARAN**

**PENUTUP**

**DAFTAR PUSTAKA**