JURNAL RESISTOR
Vol. 1 No 2 – Oktober 2108
p-ISSN 2598-7542 (Print), e-ISSN 2598-9650 (Online)
Available Online at :
http://jurnal.stiki-indonesia.ac.id/index.php/jurnalresistor

IMPLEMENTASI TEKNIK *DEEP PACKET INSPECTION* DENGAN MENGGUNAKAN WIRESHARK PADA SISTEM OPERASI UBUNTU (STUDI KASUS : INTRANET JURUSAN TEKNOLOGI INFORMASI UNIVERSITAS UDAYANA)

I Putu Agus Eka Pratama[1], Putu Adhika Dharmesta[2]

[1,2]Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana
Jl. Raya Kampus Unud, Bukit Jimbaran, Badung, Bali, Indonesia

e-mail: eka.pratama@unud.ac.id[1], adikadarmesta8@gmail.com[2]

Received : Maret, 2018	Accepted : April, 2018	Published : Oktober, 2018

Abstract

Deep Packet Inspection (DPI) is a technique commonly used by network administrator to be able to monitor in detail the flow of data in the form of data packets that occur at that moment. This data stream will produce an information that can be used for network management purposes. One example of a case study that can be done with this technique is the intranet that is available in Information Technology major Udayana University's. Deep Packet Inspection Technique is done with purpose to identifying the initial slowing down of network speed on Information Technology major Udayana University's.

***Keywords**: Deep Packet Inspection, Wireshark Linux Ubuntu, Intranet, Data Packet*

Abstrak

Deep Packet Inspection (DPI) merupakan sebuah teknik yang biasa digunakan oleh administrator jaringan untuk dapat memantau secara mendetail aliran data berupa paket data yang terjadi saat itu juga secara cepat. Aliran data ini nantinya akan menghasilkan sebuah informasi yang dapat digunakan untuk keperluan network management. Salah satu contoh studi kasus yang bisa dilakukan dengan teknik ini adalah intranet jurusan Teknologi Informasi Universitas Udayana. Teknik Deep Packet Inspection dilakukan dengan tujuan untuk identifikasi awal melambatnya kecepatan jaringan pada intranet jurusan Teknologi Informasi Universitas Udayana.

***Kata kunci**: Deep Packet Inspection, Wireshark, Linux Ubuntu, Intranet, Paket Data*

1. PENDAHULUAN

Era digital saat ini sangat bergantung kepada adanya komunikasi data yang baik antara dua buah perangkat. Perangkat ini bisa berbagai macam jenisnya mulai dari *smartphone*, PDA hingga sebuah *personal computer*. Komputer baik dalam bentuk PC dan Laptop adalah salah satu jenis perangkat yang paling banyak terkoneksi ke dalam sebuah jaringan. Jaringan yang menghubungkan berbagai jenis perangkat komputer ini sering disebut sebagai jaringan komputer. Jaringan komputer umumnya akan dibedakan menjadi empat jenis yaitu geografis, sumber data, media transmisi yang digunakan serta hubungan pada setiap komputer. Apabila dilihat berdasarkan geografisnya maka jaringan komputer dapat dibagi lagi menjadi tiga jenis yaitu LAN, MAN dan WAN. Apabila dilihat berdasarkan sumber datanya maka jaringan komputer dibagi menjadi dua yaitu

jaringan terpusat serta jaringan terdistribusi. Apabila dilihat dari media transmisinya maka jaringan komputer dibagi menjadi dua yaitu kabel dan nirkabel. Hubungan yang terjadi antara setiap komputer pada sebuah jaringan komputer dibedakan menjadi dua yaitu *client-server* serta *peer-to-peer.*

Penggunaan jaringan komputer dapat memberikan berbagai manfaat bagi penggunanya. Salah satu fungsi yang utama adalah dapat terwujudnya pengiriman data yang cepat serta efisien. Jika dibandingkan dengan metode pengiriman data yang konvensional, penggunaan jaringan komputer tentunya sangat memudahkan sekali. Hal ini disebabkan oleh penggunaan *resource* serta tenaga yang dibutuhkan jauh lebih sedikit. Sebuah jaringan komputer terkadang akan menemui suatu kendala di dalam penggunaannya. Kendala tersebut dapat berupa dari segi *physical* serta *logical* dari jaringan tersebut Untuk itu diperlukan sebuah cara untuk dapat mengidentifikasi permasalahan yang terjadi pada sebuah jaringan. *Deep packet inspection* adalah sebuah teknik untuk melakukan *network packet filtering* yang akan melakukan *scanning* terhadap *header* dan muatan dari paket data dengan menggunakan pola atau kondisi tertentu[1]. Studi kasus ini akan melakukan *capture packet data* pada intranet Teknologi Informasi Universitas Udayana lalu melakukan *filtering* dengan menggunakan tcp.analysis.retransmission. Pengaplikasian *filter* ini diharapkan mampu digunakan sebagai identifikasi awal jaringan yang mengalami penurunan kecepatan dengan melihat kegagalan retransmisi *packet* data.

2. TINJAUAN PUSTAKA

Jaringan komputer merupakan kumpulan dari beberapa *personal computer* (PC) atau *peripheral* yang saling terhubung melalui media transmisi dan melakukan akses bersama terhadap suatu *resource.* Komunikasi yang dilakukan oleh komputer tersebut dapat berupa transfer berbagai data, instruksi dan informasi dari satu komputer ke komputer lain.

Ada berbagai tipe jaringan komputer yang sering digunakan diantaranya adalah *peer-to-peer* dan *client-server.* Jaringan *peer-to-peer* memposisikan PC A dan PC B secara sama. Keuntungan penggunaan jaringan *peer-to-peer* adalah mudahnya konfigurasi, biaya operasional yang murah, dapat *sharing device* seperti harddisk, modem, fax, printer dan masih banyak lagi. Kelemahan yang dimiliki oleh jaringan ini adalah sistem keamanannya yang ditentukan oleh masing-masing *user* dengan mengatur keamanan masing-masing fasilitas yang dimiliki. Jaringan *client-server* memerlukan satu atau lebih komputer yang disebut sebagai *server* untuk mengatur lalu lintas data atau informasi dalam jaringan komputer. Komputer selain *server* yang terhubung dengan jaringan disebut sebagai *client. Server* merupakan komputer yang menyediakan fasilitas bagi komputer lain. Sedangkan *client* yaitu komputer yang menerima atau menggunakan fasilitas yang telah disediakan oleh *server. Server* dibedakan atas dua macam yaitu *dedicated server* dan *undedicated server.* Kelebihan yang dimiliki oleh jaringan *client-server* adalah terpusatnya penyedia *resource, sharing* data yang lebih efektif dan efisien, sistem keamanan dan administrasi jaringan lebih baik, serta sistem *backup* data lebih baik. Kekurangan yang dimiliki oleh jaringan *client-server* adalah biaya operasional lebih mahal, dibutuhkan satu komputer khusus yang berkemampuan lebih untuk dijadikan *server* dan tenaga *admin* yang baik, serta sangat ketergantungan pada *server.*

Apabila dilihat berdasarkan ruang lingkup dan luas jangkauannya, jaringan komputer dibedakan menjadi beberapa macam yaitu LAN, MAN dan WAN. LAN (*Local Area Network*) adalah suatu sistem jaringan dimana setiap komputer atau perangkat keras dan perangkat lunak di gabungkan agar dapat saling berkomunikasi dalam area kerja tertentu dengan menggunakan data dan program yang sama. Ruang lingkup LAN antar ruangan, gedung, kantor. MAN (*Metropolitan Area Network*) merupakan pengembangan dari LAN yang mana terdiri dari beberapa jaringan LAN yang saling berhubungan. MAN biasanya digunakan oleh sebuah perusahaan jaringan komputer dalam satu kota dan mempunyai jangkauan antara 10 Km – 50 Km. WAN (*Wide Area Network*) merupakan jaringan komputer yang terdiri dari LAN dan MAN. WAN hanya menekankan pada fasilitas kecepatan akses transmisi sehingga memungkinkan seluruh komunikasi dapat berjalan secara lancar serta efisien.

Bentuk dari sebuah jaringan komputer secara fisik dapat dibedakan menjadi beberapa topologi. Topologi tersebut diantaranya adalah topologi bus, topologi *star* dan topologi *ring*. Topologi bus adalah sebuah jaringan yang mana masing-masing server dan workstationnya dihubungkan pada sebuah kabel yang disebut dengan *backbone.* Kabel untuk menghubungkan jaringan ini biasanya menggunakan kabel Coaxial. Kelebihan pada topologi bus ini terletak pada penggunaan kabel yang sedikit dan pengembangan jaringan yang mudah. Namun terdapat pula kelemahan yang harus diperhatikan diantaranya adalah membutuhkan repeater untuk jarak jaringan yang terlalu jauh, jaringan akan terganggu apabila salah satu komputer mengalami masalah serta deteksi

kesalahan yang susah untuk dilakukan. Topologi *star* merupakan sebuah topologi yang setiap komputer pada jaringan tersebut ke sebuah pusat jaringan. Pusat jaringan ini bisa berupa *switch, hub* atau komputer lainnya. Masing-masing komputer yang terlibat tidak saling terhubung sehingga semua komunikasi harus melewati pusat jaringan terlebih dahulu. Apabila pusat jaringan ini mati maka keseluruhan jaringan akan mati pula. Kelebihan yang dimiliki oleh topologi ini adalah mudah dalam pendeteksian kesalahan karena kontrol jaringan yang terpusat, fleksibel dalam hal pemasangan jaringan baru tanpa mempengaruhi jaringan yang lain serta tidak akan bermasalah apabila satu komputer bermasalah. Terdapat pula kelemahan dari topologi ini yaitu boros dalam pemakaian kabel apabila diimplementasikan ke jaringan yang besar serta perlu penanganan khusus untuk operasional kontrolnya. Topologi *ring* adalah sebuah topologi jaringan dimana setiap komputer yang terhubung membentuk suatu lingkaran. Dengan artian setiap komputer yang terhubung ke dalam jaringan saling terkoneksi ke dua komputer lainnya sehingga membentuk sebuah cincin. Setiap komputer yang terhubung akan dijadikan sebagai *repeater.* Komputer yang diberi *frame* berhak mengirim data dan komputer yang lain menjadi *repeater.* Kelebihan dari topologi ini adalah terletak pada penggunaan kabelnya yang lebih hemat serta mampu mengisolasi kesalahan dari suatu komputer. Selain itu terdapat pula kekurangan dari topologi ini yang perlu diperhatikan yaitu sangat peka terhadap kesalahan jaringan, susah untuk dikembangkan menjadi lebih besar serta biaya pemasangannya yang mahal[8].

Deep Packet Inspection (DPI) adalah sebuah teknologi yang memungkinkan seorang yang berada pada sebuah network untuk dapat melakukan Analisa terhadap *traffic internet* yang terjadi di dalam *network* tersebut secara *real-time* dengan diferensiasi berdasarkan *payload* yang dimiliki. Teknologi DPI digunakan untuk memberikan kemampuan *network operator* untuk mengidentifikasi secara spesifik asal muasal dari setiap paket data yang melewati *network*[7]*.* Teknologi DPI juga bisa digunakan untuk meningkatkan efisiensi dari manajemen sebuah jaringan komputer. Sebagai contoh sebuah pesan yang sudah ditandai sebagai *high priority* dapat diprioritaskan untuk dikirimkan ke destinasi tujuan dibandingkan dengan pesan lainnya.

Transmission Control Protocol (TCP) adalah sebuah standar yang mendefinisikan metode untuk membuat serta menjaga sebuah jaringan sehingga sebuah aplikasi dapat saling bertukar data. TCP bekerja dengan internet protocol (IP) yang mana membantu untuk memberikan identitas kepada setiap komputer yang akan mengirimkan data. TCP akan menentukan pembagian data pada aplikasi menjadi packet yang dapat dikirimkan oleh *network* dan penerimaan packet dari *network layer* serta melakukan manajemen *flow control*. Untuk menjamin pengiriman data maka TCP akan membuat *host* pengirim untuk membuat koneksi (*connection established)* terlebih dahulu dengan *host* tujuan sebelum mengirimkan data. Ini membuat antara *host* pengirim dengan penerima dapat dipersiapkan terlebih dahulu sebelum dilakukan pengiriman data. Selama proses pengiriman data, TCP juga akan melakukan *maintenance connection*. Proses ini dilakukan dengan mengirimkan *acknowledgement* untuk *segment* yang sudah sampai di tujuan. *Acknowledgement* dikirimkan oleh *host* penerima ke *host* pengirim sebagai pemberitahuan bahwa segment sudah diterima. Karena memiliki *acknowledgment* maka TCP juga dapat menentukan untuk melakukan *retransmission segment* apabila *segment* tidak mencapai *host* tujuan.

Connection Established antara *host* pengirim dengan *host* tujuan dilakukan dengan menjalankan *three way handshake. Three Way Handshake* akan dimulai oleh *host* pengirim dengan mengirimkan *segment* yang berisikan SYN *Flag* ke *host* tujuan. Jika *host* tujuan siap dan mau melakukan komunikasi, maka host tujuan akan mengirimkan *segment* yang berisikan SYN dan ACK *Flag.* Bila *host* tujuan tidak mau melakukan komunikasi, maka yang dikirimkan adalah *segment* dengan *Flag* RST, ACK. Bila *host* tujuan tidak ada , maka tidak aka nada balasan sama sekali. Teknik ini memungkinkan *host* pengirim untuk dapat membedakan beberapa kondisi yaitu ada tidaknya host tujuan dan mau tidaknya host tujuan melakukan komunikasi. Tahapan terakhir adalah pengiriman *segment* yang berisi *flag* ACK kepada *host* tujuan. Selama proses pengiriman data, host tujuan akan mengirimkan *acknowledgment* sebagai tanda bahwa *segment* sudah tiba ditujuan. *Acknowledment* tidak dikirimkan untuk setiap *segment,* namun dikirimkan untuk sejumlah *segment.* Sejumlah *segment* tersebut disebut dengan *Window Size*.

Jika pengiriman data sudah selesai, maka TCP akan melakukan *Terminate Connection*. Host yang menganggap pengiriman telah selesai akan memulai proses *Terminate Connection*. *Terminate Connection* dilakukan dengan mengirimkan *segment* dengan *flag* FIN dan akan dibalas dengan *flag* ACK. Untuk sebuah komunikasi dibutuhkan empat *segment,* baik FIN maupun ACK dari kedua sisi *host*.

Segment dari sebuah pengiriman data memiliki ISN (*Initial Sequence Number*) yang dapat menunjukan urutan setiap s*egment* pada *stream* data. Karena pengiriman *segment* TCP dapat menempuh jalur yang berbeda-beda untuk setiap *segment,* maka *host* tujuan harus mampu mengurutkan kembali setiap *segment* yang diterimanya.

TCP memiliki berbagai *flag* yang digunakan sebagai parameter untuk mengontrol kondisi yang sedang terjadi. Parameter tersebut adalah SYN, FIN dan ACK[3]. Setiap *bit* data yang dikirmkan oleh koneksi TCP memiliki urutan nomor yang berasosiasi. TCP *retransmission* akan memastikan data yang terkirim dapat terjaga dengan baik. Apabila *retransmission* terdeteksi dalam sebuah koneksi TCP, secara logika dapat diasumsikan bahwa *packet loss* terjadi pada antara *client* dengan *server* pada sebuah jaringan[4].

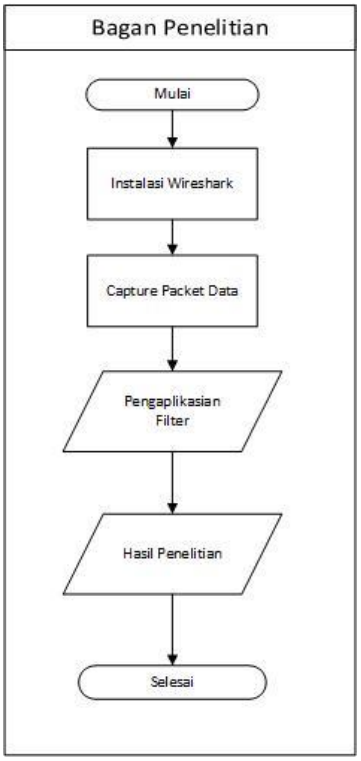
Untuk lebih menambah pemahaman, maka refrensi yang digunakan adalah mengambil dari refrensi penelitian dan juga buku yang sebelumnya telah melakukan pembahasan mengenai topik ini. Penambahan refrensi ini akan membantu dalam melakukan penelitian ini. Hasil yang didapatkan pada penelitian sebelumnya dapat dijadikan referensi dalam mengerjakan penelitian ini.

Referensi penelitian yang dilakukan oleh I Putu Agus Eka Pratama dalam bukunya yang berjudul Handbook Jaringan Komputer – Teori dan Praktik Berbasiskan *Open Source* menjelaskan penggunaan *Deep Packet Inspection* pada wireshark dalam sistem operasi Linux Ubuntu untuk melakukan *filtering* hasil *capture* jaringan dengan tujuan melihat *packet* data dengan destinasi IP 192.168.1.7 serta melihat perincian yang ada pada setiap paket data[6].

Penelitian yang dilakukan oleh Faizal Eko Nugroho dalam jurnalnya yang berjudul Analisis Perbandingan Perfomansi *Deep Packet Inspection Firewall* Antara L7-Filter dan n-DPI menjelaskan penggunaan *Deep Packet Inspection* sebagai metode yang diaplikasikan pada L7-filter dan nDPI dalam menguji nilai sensitifitas dan spesifitas pada studi kasus yang diberikan[5].

3. METODOLOGI PENELITIAN

Metodologi penelitian akan dimulai dengan melakukan instalasi aplikasi wireshark terlebih dahulu pada sistem operasi Linux Ubuntu 16.04. Kemudian dilanjutkan dengan proses *capture packet data* pada *interface* jaringan yang dipilih. Jaringan yang akan digunakan untuk melakukan proses capture serta analisa adalah jaringan intranet Teknologi Informasi Universitas Udayana. Begitu *interface* dari jaringan sudah dipilih maka lakukan proses *capture* untuk merekam aktivitas dari jaringan tersebut. Nantinya akan muncul serangkaian *list* yang menampilkan *packet* data yang melewati jaringan tesebut. Setelah serangakaian *list packet* data terlihat, penelitian dilanjutkan dengan melakukan *filtering* terhadap *packet* data tersebut. Filtering berguna untuk menyaring serangkaian *packet* data yang terlihat menjadi beberapa *packet* data yang hanya ingin dianalisa saja. *Filter* yang digunakan adalah tcp.analysis.retransmissions. *Filter* ini digunakan untuk melihat *packet* data mana yang telah hilang pada komunikasi antara *client* dengan *server*. Studi kasus yang diangkat adalah intranet Teknologi Informasi Universitas Udayana, dimana penelitian akan melihat pada saat mengakses apa pengguna dalam jaringan tersebut mengalami tcp *retransmission*. Untuk melakukan identifikasi awal terhadap jaringan yang lambat dilakukan pengecekan terhadap nilai RTO dari *packet* data yang masuk ke dalam kategori tcp *retransmission.*



Gambar 1 Bagan Metode Penelitian

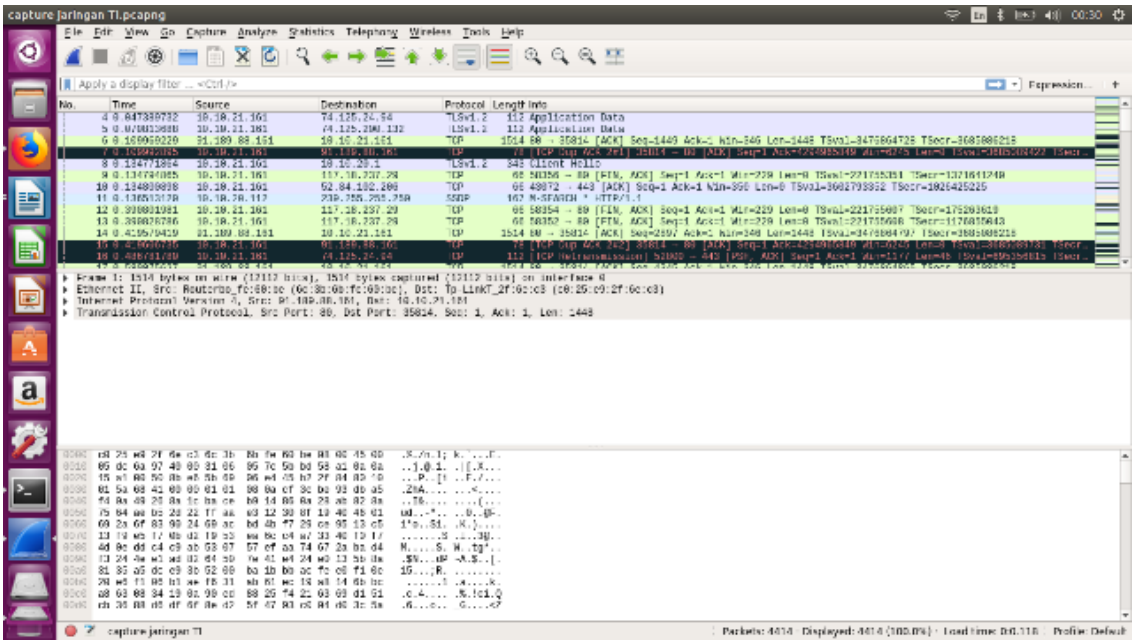
4. HASIL PENELITIAN

Berikut ini merupakan pembahasan mengenai hasil penelitian yang dilakukan dengan berdasrkan metodologi penelitian yang telah dijelaskan sebagai berikut

4.1 Buka Wireshark Dan Lakukan Capture Network

Untuk membuka wireshark pada ubuntu pastikan untuk merubah hak akses *user* menjadi *superuser* lalu gunakan sintak wireshark pada *terminal*. Setelah itu pilih *network interface* yang terhubung pada jaringan intranet Teknologi Informasi Universitas Udayana. Jaringan inilah yang akan dianalisa untuk dilihat mengenai aktivitas yang terjadi di dalamnya.

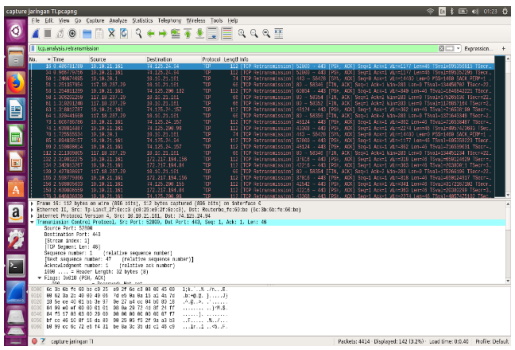
Gambar 2 memperlihatkan hasil *capture* yang dilakukan pada jaringan intranet Teknologi Informasi dengan menggunakan tool wireshark pada sistem operasi Linux. Terlihat pada gambar bahwa terdapat sekumpulan packet data yang melewati jaringan intranet Teknologi Informasi ini. Packet ini mengandung sekumpulan data yang berasal dari perangkat komputer yang terkoneksi dalam jaringan. Packet data ini dapat memberikan informasi seputar jaringan tersebut.



Gambar 2 Hasil Capture Intranet Teknologi Informasi

4.2 Lakukan Filtering Dengan Tcp Retramissions

Aplikasikan filter tcp.analysis.retramissions pada hasil *capture* pada jaringan intranet Teknologi Informasi Universitas Udayana. *Filter* ini akan menampilkan *packet* data apa saja yang melakukan *retransmission* karena *packet* yang dikirim sebelumnya tidak memberikan timbal balik berupa TCP ACK *Packet*[2]. Apabila *retransmission* dilakukan melebihi jumlah yang di konfigurasi sebelumnya maka ada kemungkinan terjadinya masalah antara komputer pengguna dengan jaringan yang digunakan.



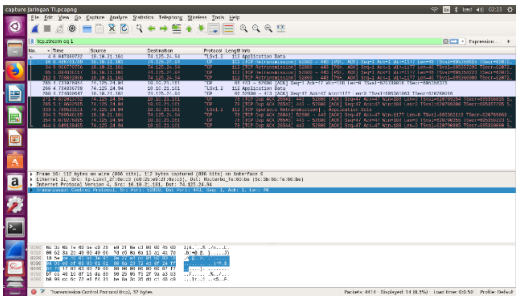
Gambar 3 Filter tcp.analysis.retramissions

Gambar 3 memperlihatkan tampilan pada hasil *capture* jaringan intranet Teknologi Informasi Universitas Udayana pada Wireshark yang sudah menggunakan filter tcp.analysis.retramissions. Apabila diperhatikan dengan baik terdapat beberapa packet data dengan status *retransmission timeout.* Hal ini menandakan bahwa ada beberapa packet yang gagal untuk

di transmisi kembali. Gagalnya retransmisi ini umumnya men

4.3 Follow Tcp Stream Pada Sebuah Packet Data

Follow TCP *stream* digunakan untuk mengikuti aliran dari paket data TCP yang dilakukan. Proses *follow* tcp *stream* ini akan membuat paket TCP tersebut terlihat asal mulanya. Untuk melakukan TCP *stream* klik kanan pada *packet* yang diinginkan lalu pilih *follow* kemudian akan muncul *list packet* data yang berkaitan dengan TCP ini

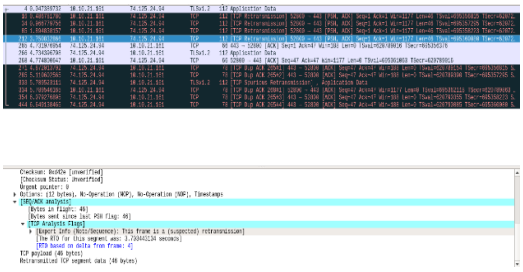


Gambar 4 *Follow* TCP *Stream* pada *Packet Data*

Gambar 4 merupakan tampilan dari wireshark pada saat sebuah *packet* data dilacak keberadaan TCP *stream*-nya. Terlihat serangkaian TCP yang mengawali *packet* data tersebut. Beberapa TCP yang mengawali sudah terlihat memiliki *retransmission timeout*.

4.4 Lihat Rto Dari Packet Data

RTO merupakan retransmission timeout yang digunakan untuk melihat waktu yang diperlukan oleh sebuah TCP untuk melakukan acknowledge terhadap dua buah komputer yang sedang terhubung. Apabila waktu RTO yang ditampilkan maka akan mempengaruhi respon dari dua buah komputer yang sedang terhubung tersebut. Hal ini dikarenakan komputer pengirim harus menerima acknowledge dari komputer penerima terlebih dahulu untuk dapat melanjutkan proses komunikasi.



Gambar 5 Nilai RTO pada *Packet* Data

Terlihat pada gambar bahwa paket data dengan no 212 memiliki nilai RTO yang cukup besar yaitu sebesar 3,7 *seconds*. Hal ini bisa menjadi indikasi bahwa terjadi permasalahan kecepatan akses dari dan menuju komputer yang tertera pada IP *address.*

5. SIMPULAN

Simpulan yang dapat ditarik dari proses penelitian ini bahwa teknik *deep packet inspection* mampu digunakan untuk melihat detail dari sebuah *packet* data yang melakukan transmisi pada suatu jaringan dengan mendetail serta dapat dimanfaatkan untuk berbagai keperluan. *Deep packet inspection* mampu menangkap *packet* data yang memiliki TCP *retransmission*. Setiap *packet* yang sudah difilterisasi dengan TCP *retransmission* juga memiliki beberapa info tambahan yang mana salah satunya adalah RTO. RTO dapat dijadikan sebagai pendeteksi dini terhadap melemahnya koneksi jaringan akibat hilangnya *packet* data yang dikirimkan dan diterima.

DAFTAR PUSTAKA

[1] Barak, Lior. "*Implementing a prototype for the Deep Packet Inspection as a Service Framework*." M.Sc. Efi Arazi School of Computer Science, 2016

[2] Sanders, Chris. *Practical Packet Analysis, 2nd Edition*., San Francisco: No Starch Press, 2011

[3] Strecth, Jeremy. "Understanding TCP Sequence and Acknowledgment Numbers." Internet: http://packetlife.net/blog/2010/jun/7/understanding-tcp-sequence-acknowledgment-numbers/, 7Juni 2010 [01 Mei 2018]

[4] Greer, Chirs. “Network Packet Loss, Retransmissions, and Duplicate Acknowledgements.” Internet: https://www.performancevision.com/blog/network-packet-loss-retransmissions-and-duplicate-acknowledgements/, 14 Juni 2017 [01 Mei 2018].

[5] Eko Nugroho, Faizal. “*Analisis Perbandingan Perfomansi Deep Packet Inspection Firewall Antara L7-Filter dan n-DPI,*” *e-Proceeding of Engineering*., vol. 2 no. 1 pp.1469 April 2015

[6] I Putu Agus Eka Pratama. *Handbook Jaringan Komputer – Teori dan Praktik Berbasiskan Open Source.,* Bandung: Informatika Bandung, 2015

[7] TEC. “White Paper on Deep Packet Inspection.” Internet: http://tec.gov.in/pdf/Studypaper/White%20paper%20on%20DPI.pdf, 20 November, 2011 [10 Mei 2018].

[8] Wahyudi, Didik R. “Modul Praktikum Jaringan Komputer”. Universitas Islam Negeri Sunan Kalijaga, 2015