

IMPLEMENTASI WIRESHARK DALAM MELAKUKAN PEMANTAUAN PROTOCOL JARINGAN

(Studi Kasus : Intranet Jurusan Teknologi Informasi Universitas Udayana)

I Putu Agus Eka Pratama¹, Putu Adhika Dharmesta²

^{1,2} **Teknologi Informasi,**

Fakultas Teknik, Universitas Udayana Denpasar, Jl. P.B. Sudirman, Kota Denpasar, Bali 80234

e-mail: eka.pratama@unud.ac.id¹, adikadarmesra8@gmail.com²

Abstract

Wireshark is a leading open source tool that is widely used to analyze and troubleshoot network problems, allowing us to find out about network problems. The development of Wireshark evolved thanks to the contribution of volunteer network experts around the world and is a continuation of the project started by Gerald Combs in 1998. This monitoring covers the flow of protocol that is being used by networks and computers. This test will implement Wireshark as an application to monitor computer communication networks to see and process the results of network monitoring with case studies on the intranet of the Information Technology Department of the Faculty of Engineering, Udayana University

Keywords: *Wireshark, Linux, Protocol, Intranet, Packet Capture*

Abstrak

Wireshark adalah tool open source terkemuka yang banyak di gunakan untuk melakukan analisis dan pemecah masalah jaringan, Memungkinkan kita untuk mengetahui masalah di jaringan. Pengembangan Wireshark berkembang berkat kontribusi relawan ahli jaringan di seluruh dunia dan merupakan kelanjutan dari proyek yang dimulai oleh Gerald Combs pada tahun 1998. Pemantauan ini mencakup alur protocol yang sedang digunakan oleh jaringan dan komputer tersebut. Pengujian ini akan menerapkan wireshark sebagai sebuah aplikasi pemantauan jaringan komunikasi computer untuk melihat dan mengolah hasil pemantauan jaringan dengan studik kasus di intranet jurusan Teknologi Informasi Fakultas Teknik Universitas Udayana

Kata Kunci: *Wireshark, Linux, Protocol, Intranet, Packet Capture*

1. Pendahuluan

Di tengah semakin kerasnya perkembangan digitalisasi yang saat ini tengah berlangsung dalam segala aspek kehidupan masyarakat saat ini, komunikasi jaringan komputer memegang peranan yang penting di dalamnya. Komunikasi ini dapat dilakukan dari berbagai perangkat komputasi yang ada asalkan sudah terhubung pada sebuah jaringan yang sama. Jaringan computer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumberdaya (printer, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban web). Tujuan dari jaringan computer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan computer dapat meminta dan memberikan layanan (service). Pihak yang meminta/menerima layanan disebut klien (client) dan yang memberikan/mengirim layanan disebut peladen (server). Desain ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Jaringan yang digunakan untuk menghubungkan perangkat ini dapat berupa wireless ataupun wired. Jaringan wired akan menghubungkan satu computer dengan komputer lain diperlukan penghubung berupa kabel jaringan. Kabel jaringan berfungsi dalam mengirim informasi dalam bentuk sinyal listrik antar computer jaringan. Sedangkan pada jaringan wireless menggunakan medium berupa gelombang elektro magnetic sebagai media penghantarnya. Pada jaringan ini tidak diperlukan kabel untuk menghubungkan antar computer karena menggunakan gelombang elektro magnetik yang akan mengirimkan sinyalin formasi antar computer jaringan.

Dalam melakukan sebuah komunikasi antara dua buah perangkat atau lebih pada sebuah jaringan computer diperlukan adanya standarisasi komunikasi agar semua perangkat dapat memahami apa yang sedang dikomunikasikan. Berangkat dari permasalahan tersebut muncul istilah protokol. Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan

data antara dua atau lebih titik komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya.

Pada tingkatan yang terendah, protocol mendefinisikan koneksi perangkatkeras. 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 beberapa jenis jaringan komputer apabila dilihat berdasarkan cakupan wilayah yang dijangkauanya. Jenis-jenis jaringan komputer tersebut diantaranya adalah PAN, LAN, MAN, WAN dan Internet. PAN merupakan jaringan yang menghubungkan antar dua device atau lebih dalam jarak yang dekat (10 meter atau kurang). PAN dapat digunakan untuk komunikasi perangkat personal seperti PDA ke laptop, dll. Salah satu teknologi dari PAN adalah Bluetooth. Bluetooth dapat menghubungkan 7 device dalam satu jaringan, seperti menghubungkan mouse dengan laptop, printer dengan laptop dan sejenisnya. LAN merupakan jaringan yang memiliki area yang kecil. Cakupan area LAN terbatas hanya dalam satu kantor atau satu bangunan saja (contoh: satu perusahaan). LAN menghubungkan antar device seperti Laptop, PC, server, printer, dll. Biasanya user pada jaringan LAN dapat mengakses device lain atau server pada jaringan tersebut. Dalam suatu perusahaan, terdapat karyawan yang memiliki hak khusus untuk akses informasi penting. Jika terdapat celah keamanan pada LAN, maka akan memungkinkan attacker menyisipkan sebuah ancaman keaman terhadap celah tersebut. Jika attacker masuk ke celah tersebut dan menjadi user yang memiliki hak akses, maka attacker dapat mengubah atau mencuri informasi dari perusahaan tersebut. MAN merupakan jaringan yang mencakup suatu daerah atau kota. MAN terdiri dari gabungan beberapa LAN. MAN memiliki transfer data berkecepatan tinggi yang menghubungkan berbagai lokasi, contoh: kampus, fasilitas umum (rumah sakit, apotek, dll), pemerintahan, dll. Ancaman keamanan terhadap informasi MAN sama seperti LAN tetapi dalam skala yang besar. Sehingga pengaksesan informasi penting memiliki autentikasi yang lebih banyak dan aman. WAN memiliki cakupan area yang lebih luas dibandingkan dengan LAN dan MAN. WAN dapat mencakup suatu Negara, antar lokasi atau pulau. WAN sangat penting untuk beberapa perusahaan besar. Internet mencakup jaringan yang dapat terhubung ke seluruh dunia. Internet menjadikan pengaksesan informasi, komunikasi,

transfer file menjadi lebih mudah dan cepat. Terkadang internet juga dimanfaatkan untuk memperoleh penghasilan.

Agar dapat terhubung ke jaringan internet, kita membutuhkan sebuah Internet Service Provider (ISPs). ISPs akan menyediakan akses jaringan LAN, MAN, WAN yang terhubung ke seluruh dunia. Dalam hal ini ISPs menggunakan point-of-presence (POP), atau biasa disebut access point (NAP). ISPs juga menangani traffic yang terhubung ke ISPs lain. Semakin besar cakupan jaringannya maka semakin banyak juga serangan yang diterima^[2].

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*^[3].

Pengaplikasian jaringan pada suatu daerah nantinya akan membutuhkan sebuah topologi dalam merancang jaringan di dalamnya. Topologi Jaringan komputer adalah metode atau cara yang digunakan agar dapat menghubungkan satu komputer dengan komputer lainnya. Struktur atau jaringan yang digunakan untuk menghubungkan satu komputer dengan komputer lainnya bisa dengan menggunakan kabel ataupun nirkabel (tanpa kabel). Pada pelaksanaannya, ada beberapa macam topologi jaringan komputer yang digunakan sesuai dengan skala jaringan, tujuan, biaya, dan penggunaanya. Beberapa macam topologi jaringan

tersebut adalah topologi ring, topologi bus, topologi star, topologi mesh, dan topologi tree. Masing-masing jenis topologi tersebut memiliki kelebihan dan kekurangan sehingga dalam penggunaannya harus benar-benar memperhatikan peruntukannya. Topologi ring atau sering disebut dengan topologi cincin merupakan suatu topologi jaringan yang dipakai untuk menghubungkan sebuah komputer dengan komputer lainnya dalam sebuah rangkaian yang berbentuk melingkar seperti cincin. Jenis topologi jaringan ini umumnya hanya menggunakan LAN card agar masing-masing komputer terkoneksi. Topologi bus adalah topologi jaringan yang lebih sederhana. Pada umumnya topologi jaringan ini dilakukan pada instalasi jaringan berbasis kabel coaxial. Topologi bus memakai kabel coaxial pada sepanjang node client dan konektor. Jenis konektor yang digunakan adalah BNC, Terminator, dan TBNC. Topologi star atau disebut juga dengan topologi bintang adalah topologi jaringan berbentuk bintang dimana pada umumnya memakai hub atau switch untuk koneksi antar client. Topologi jaringan komputer ini paling sering digunakan saat ini karena memiliki banyak kelebihan. Topologi mesh adalah sebuah topologi yang bisa digunakan untuk rute yang banyak. Jaringan pada topologi ini menggunakan kabel tunggal sehingga proses pengiriman data menjadi lebih cepat tanpa melalui hub atau switch. Topologi tree atau topologi pohon adalah hasil penggabungan dari topologi bus dan topologi star. Topologi tree pada umumnya dipakai untuk interkoneksi antara hirarki dengan pusat yang berbeda-beda. Topologi peer to peer adalah topologi jaringan yang sangat sederhana karena hanya menghubungkan 2 komputer. Pada umumnya topologi peer to peer memakai satu kabel saja untuk menghubungkan kedua komputer agar bisa saling berbagi data. Topologi linier atau sering disebut dengan topologi bus berurut. Topologi ini umumnya hanya memakai satu kabel utama sebagai konektor masing-masing titik sambungan pada setiap komputer. Topologi Hybrid adalah gabungan dari beberapa topologi yang berbeda dan membantu jaringan baru. Dengan kata lain, jika ada dua atau lebih topologi yang berbeda terhubung dalam satu jaringan maka topologi jaringan tersebut akan membentuk topologi hybrid^[1]. Komunikasi yang dilakukan pada sebuah jaringan komputer memerlukan adanya sebuah kesepakatan antar komputer untuk dapat saling berkomunikasi dengan baik. Kesepakatan ini sering disebut sebagai protocol. Dalam dunia jaringan dan internet, protokol sendiri diartikan sebagai sebuah aturan atau standar yang mengatur dan memungkinkan terjadinya hubungan komunikasi dan

perpindahan data dari satu ke dua atau lebih komputer. Protokol ini pun dapat diterapkan pada perangkat keras dan perangkat lunak atau kombinasi dari keduanya.

Ada berbagai jenis protocol yang sering digunakan dalam jaringan dan internet diantaranya adalah TCP/IP, Ethernet, UDP, RTP, FTP, HTTP, DHCP, DNS, ICMP, IMAP, HTTPS, SSH, dan SSL.

TCP/IP adalah standar komunikasi data yang digunakan oleh komunitas internet untuk proses tukar-menukar data dari satu komputer ke komputer lain dalam jaringan internet. Protokol ini tidak dapat berdiri sendiri tanpa bantuan komponen lain, dikarenakan TCP/IP sendiri hanya berfungsi sebagai pembungkus protokol (protocol suite). Ethernet sering digunakan untuk menghubungkan komputer ke internet. Ethernet sendiri menggunakan metode akses yang disebut dengan CSMA/CD (Carrier Sense Multiple Access/Collision Detection). CSMA/CD ini adalah sebuah sistem yang mana mengharuskan setiap komputer untuk menunggu instruksi jaringan sebelum dapat mengirimkan data atau informasi ke komputer lain. Dalam hal ini, jika jaringan tidak sibuk, barulah komputer tersebut akan menyampaikan informasi atau data. Namun apabila ternyata jaringan sibuk, maka komputer otomatis akan menunggu hingga jaringan mengizinkan atau istilahnya sampai jaringan tidak sibuk. UDP merupakan salah satu protokol yang berada pada lapisan TCP/IP, dan dapat mendukung komunikasi yang tidak andal (unreliable). Tidak andal yang dimaksud disini adalah tanpa koneksi. Jadi, protokol UDP memiliki kemampuan untuk menghubungkan komputer bahkan tanpa adanya koneksi TCP/IP sekalipun. RTP atau Real Time Protocol adalah salah satu protokol jaringan yang menyediakan fungsi untuk mengantarkan data secara real time. Seperti misalnya data audio, video, dan lain-lain biasanya data dapat dikirim melalui layanan jaringan multicast atau layanan unicast. FTP biasa digunakan untuk melakukan unggah maupun unduh file. Keamanannya sendiri didasarkan pada username dan password yang dibuat komputer, namun terkadang tidak sedikit juga anonymous diperbolehkan login. HTTP merupakan protokol yang sudah tidak asing lagi dan umumnya kerap digunakan untuk melakukan transfer halaman web. Namun sebelum adanya teknologi HTTP ini, para webmaster tempo lalu rupanya menggunakan protokol Gopher. Tapi sayangnya, protokol Gopher hanya mendukung text saja, sehingga dinilai tidak efektif untuk melakukan transfer dan download halaman website. DHCP merupakan protocol berfungsi untuk memberikan alamat Internet Protocol (IP) secara otomatis apabila komputer tersambung dengan cable-connection yang berasal dari ISP. DNS merupakan

protokol jaringan dan biasa digunakan pada aplikasi yang terhubung ke jaringan internet, misalnya seperti peramban internet, email, dan aplikasi lainnya. DNS ini juga dapat membantu memetakan hostname dari sebuah komputer ke IP address.

ICMP merupakan sebuah protocol yang memiliki fungsi yang sedikit berbeda dari TCP atau UDP dari segi penggunaannya. Sebab protokol ini tidak dapat digunakan secara langsung oleh aplikasi jaringan milik pengguna. Umumnya, ICMP kerap digunakan oleh sistem operasi komputer untuk memberikan pemberitahuan bahwa komputer yang dituju tidak bisa dijangkau. IMAP merupakan protokol standar yang digunakan untuk mengakses atau mengambil email dari server. IMAP memungkinkan pengguna untuk memilih pesan email yang akan diambil, mencari pesan e-mail tertentu, bahkan menghapus pesan email yang ada. Kemampuan yang dimiliki IMAP lebih baik ketimbang POP (Post Office Protocol) yang mengizinkan penggunaanya mengambil dan mengunduh semua pesan yang ada tanpa kecuali. HTTPS merupakan protocol yang termasuk dalam bagian dari WWW (World Wide Web) dan ditemukan oleh Netscape Comumunications Corporation yang menyediakan autentikasi dan komunikasi tersandi untuk penggunaan dalam komersi elektrik. Dalam pembentukannya, HTTPS menggunakan berbagai macam teknologi komunikasi seperti plain text, dan SSL (Security Socket Layer). Kedua teknologi tersebut memberikan perlindungan yang memadai dari serangan eavesdroppers dan man in the middle attacks. SSH atau Sucur Shell adalah protokol jaringan yang memungkinkan penggunaanya melakukan pertukaran data secara aman antara dua komputer atau lebih. SSH umumnya secara fungsi digunakan untuk mengendalikan informasi dari jarak jauh seperti menerima dan mengirim file. Penggunaan protokol ini juga harus menggunakan Tunnel yang terenskripsi. Adapun kelebihan SSH dibandingkan dengan protokol Telnet, FTP, dan RSH adalah karena SSH sendiri memiliki sistem otentikasi, otorisasi, dan enkripsinya sendiri. SSH juga dipercayai membuat keamanan komunikasi menjadi lebih terjamin. SSL merupakan salah satu protokol yang paling banyak digunakan, terlebih untuk meningkatkan keamanan website dan protokol ini juga digadang-gadang memiliki kemampuan enkripsi tingkat tinggi. Tidak hanya mampu mengamankan website saja, SSL rupanya serta dapat memberikan pengamanan lebih untuk aplikasi yang memerlukan enkripsi jaringan end-to-end^[4].

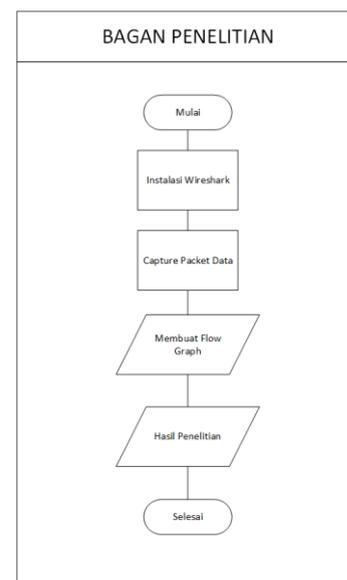
2. Metode Penelitian

Metodologi penelitian akan dimulai dengan melakukan instalasi aplikasi wireshark terlebih dahulu pada system operasi Linux Ubuntu 19.04. 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 dilakukan proses capture untuk merekam aktivitas dari jaringan tersebut. Nantinya akan muncul serangkaian list yang menampilkan packet data yang melewati jaringan tersebut. Setelah serangkaian data tersebut berhasil ditampilkan langkah selanjutnya adalah dengan melihat pada menu `statistic>flow graph`. Nantinya akan muncul diagram aliran data beserta protocol yang digunakan pada suatu komunikasi pada sebuah jaringan. Studi kasus jaringan yang digunakan adalah jaringan intranet pada Jurusan Teknologi Informasi Fakultas Teknik Universitas Udayana.

2.1 Tahapan Penelitian

Berikut merupakan tampilan bagan untuk tahapan penelitian.



Gambar 1. Bagan Tahapan Penelitian

Berdasarkan bagan pada gambar 1, tahapan penelitian dimulai dari instalasi wireshark pada system operasi Ubuntu. 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.

2.2 Analisa Kebutuhan Perangkat

Berikut merupakan kebutuhan perangkat

untuk penelitian yang meliputi perangkat keras dan perangkat lunak.

2.2.1. Perangkat Keras

Perangkat keras yang digunakan adalah 1 (satu) buah laptop Dell Inspiron 7447 dengan spesifikasi sebagaiberikut.

- 1) Prosesor Intel Core i7-4700HQ
- 2) RAM8GB.
- 3) Harddisk1TB.

2.2.3. Perangkat Lunak

Perangkat lunak yang digunakan untuk penerapan proxy server adalah sebagaiberikut.

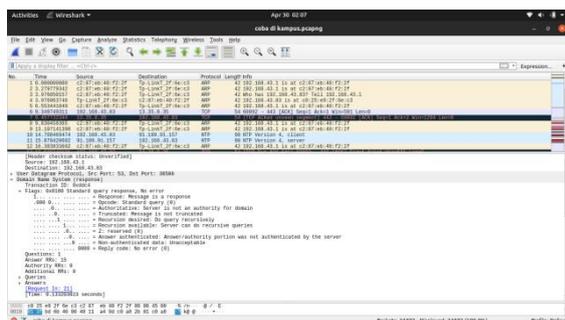
- 1) Sistem operasi Ubuntu 19.04
- 2) Wireshark

3. Hasil dan Pembahasan

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

3.1 Buka Wireshark dan Lakukan Packet Capture

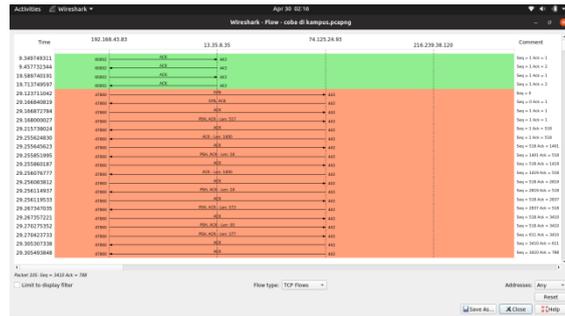
Untuk membuka wireshark pada ubuntu pastikan untuk merubah hak akses user menjadi superuser lalu gunakan sintak wireshark pada terminal. Setelah itu pilih network interface yang terhubung pada jaringan intranet Teknologi Informasi Universitas Udayana. Jaringan inilah yang akan dianalisa untuk dilihat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



Gambar 2 Hasil Packet Capture

3.2 Lihat Flow Graph Protocol

Flow graph digunakan untuk melihat aliran data yang terjadi pada sebuah komunikasi jaringan. Untuk melihat flow graph pada wireshark pengguna dapat mengklik `statistic>flow graph` pada menu bar wireshark.



Gambar 3 Aliran data TCP

Gambar diatas merupakan aliran data yang dilakukan oleh protocol TCP. Dalam TCP dikenal dengan sebuah proses 3-way handshake. Proses komunikasi ini dilakukan antara dua perangkat melalui internet dengan menggunakan model TCP/IP. Proses ini dituju kanuntuk memastikan koneksi yang terhubung antara client dan server sudah terjadi dengan baik. Gambar dari flow graph memperlihatkan proses yang terjadi tersebut. Dimana kita bisamelihat komunikasi yang terjadi antara perangkat dengan ip 192.168.43.83 dengan perangkat dengan IP 74.125.24.93. Langkah pertama perangkat dengan ip local membentuk koneksi dengan server pada ip public dengan mengirimkan segment yang berisi SYN (Synchronize Sequence Number) yang mana akan menginformasikan server yang ingin dikoneksikan dengan client. Kemudian server akan merespon dengan mengirimkan sinyal SYN-ACK. ACK (acknowledgement) mengindikasikanrespondari segment yang diterima sebelumnya dan SYN mengindikasikan sequence number berapa segment akan dimulai. Yang terakhir client akan menganalisisrespon dari server yang kemudianakan membentuk koneksi yang stabil yang nantinya akan digunakan untuk bertukar data yang sesungguhnya.

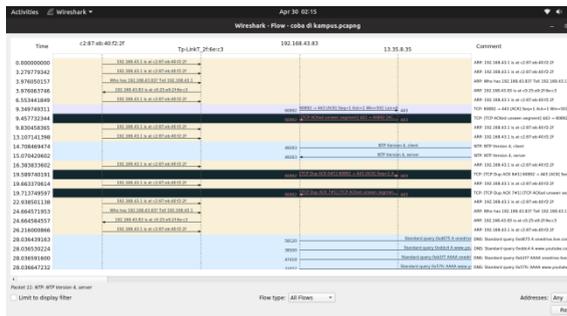


Gambar 4 Aliran Data Protocol DNS

Gambar diatas merupakan tampilan dari flow graph yang memperlihatkan aliran data dari protocol DNS. Protocol ini bias dikatakan merupakan buku teleponnya internet. Sebenarnya untuk berinteraksi dengan sebuah website, sebuah web browser harus berkomunikasi menggunakan ip address dari server

website tersebut berada.

Namun untuk dapat mengingatkan ip address dari setiap website yang ingin dicari tentunya tidaklah mudah. Untuk itu diperlukan DNS sebagai sebuah protocol yang mampu menerjemahkan nama domain menjadi IP address dari server tempat website itu berada. Seperti terlihat pada gambar bahwa jaringan pertama kali akan melakukan mengirimkan paket standard query kepada dns server. Standard query inberisikan transaction id dan juga query yang dimasukan oleh pengguna. Nantinya server akan memberikan response dari hasil query yang diberikan.



Gambar 5 Aliran Data Protocol ARP

Gambar diatas merupakan tampilan dari flow graph yang memperlihatkan aliran data protocol ARP. Protocol ARP atau Address Resolution Protocol merupakan sebuah protocol yang bertanggungjawab untuk mencari tahu MAC Address atau alamat hardware dari suatu host yang tergabung dalam sebuah jaringan LAN dengan memanfaatkan IP Address yang sudah terkonfigurasi.

4. Kesimpulan

Simpulan yang dapat ditarik dari penelitian yang dilakukan adalah bahwa dalam melakukan pemantauan protocol jaringan dapat dilakukan dengan memanfaatkan aplikasi wireshark yang terinstall pada system operasi Ubuntu. Untuk melihat bagaimana sebuah packet data dengan protocol tertentu bergerak pengguna bias melihat flow graph yang sudah ada pada wireshark.

5. Referensi

- [1] Maxmanroe. “Pengertian, Jenis, dan Gambar Topologi Jaringan” Internet: <https://www.maxmanroe.com/vid/teknologi/komputer/topologi-jaringan.html>, 8 Januari 2018 [01 Mei 2019]
- [2] Wahyuningsih. “Berbagai Tipe Jaringan Komputer” Internet: <https://netsec.id/jaringan-komputer/>, 2 Februari 2017 [03 Mei 2019]
- [3] I Putu Agus Eka Pratama. Handbook Jaringan Komputer – Teori dan Praktik Berbasis Open Source., Bandung: Informatika Bandung, 2015
- [4] Sanders, Chris. Practical Packet Analysis, 2nd Edition., San Francisco: No Starch Press, 2011