JARINGAN KOMPUTER

( Visualisasi PCAP )



Nama : Rahmi Khoirani

NIM : 09011281520104

Kelas : SK 5C

Dosen Pengampuh : Deris Stiawan, M.T., Ph.D.

Jurusan Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2017

**BAB I**

**PENDAHULUAN**

1. **Latar Belakang**

Jaringan komputer bukanlah sesuatu yang baru saat ini, hampir disetiap tempat terdapat jaringan komputer untuk memperlancar arus informasi pada tempat tersebut. Didalam sebuah jaringan komputer terdapat banyak sekali paket data yang berlalu lalang pada kabel jaringan, baik itu paket data yang mengandung informasi informasi seperti password, alamat sebuah situs, user name, dan lainlain. Paket data tersebut juga dapat menggambarkan keadaan pada sebuah jaringan komputer.

Wireshark merupakan salah satu network analysis tool, atau disebut juga dengan protocol analysis tool atau packet sniffer. Wireshark dapat digunakan untuk troubleshooting jaringan, analisis, pengembangan software dan protocol, serta untuk keperluan edukasi. Wireshark merupakan software gratis, sebelumnya, Wireshark dikenal dengan nama Ethereal.

1. **Rumusan Masalah**
2. Apa yang di maksud dengan wireshark?
3. Apa saja fungsi wireshark?
4. Bagaimana visualisasi wireshark?
5. **Tujuan**
6. Mengetahui pengertian wireshark.
7. Mengetahui fungsi-fungsi wireshark.
8. Mengetahui visualisasi wireshark.

**BAB II**

**ISI**

1. **Pengertian Wireshark**

Wireshark adalah penganalisa paket bebas dan open source. Hal ini digunakan untuk troubleshooting jaringan, analisis perangkat lunak, dan pengembangan protokol komunikasi serta pendidikan. Awalnya bernama Ethereal, tetapi pada Mei 2006, proyek ini berganti nama Wirwshark karena masalah merk dagang. Wireshark adalah cross-platform, menggunakan GTK + widget toolkit untuk mengimplementasikan antarmuka pengguna, dan menggunakan pcap untuk menangkap paket, itu berjalan pada berbagai Unix-seperti sistem operasi termasuk Linux, Mac OS X, BSD, dan Solaris, dan pada Microsoft Windows. Ada juga berbasis terminal (non-GUI) versi yang disebut TShark. Wireshark, dan program lain yang didistribusikan dengan itu seperti TShark, adalah perangkat lunak bebas, dirilis di bawah ketentuan GNU General Public License.

Wireshark merupakan salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya terrmasuk protokol didalamnya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis. Wireshark mampu menangkap paket-paket data atau informasi yang banyak dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting seperti password email atau account lain) dengan menangkap paket-paket yang banyak di dalam jaringan dan menganalisanya sedetail mungkin.

1. **Fungsi Wireshark**

Wireshark dipakai oleh network administrator untuk menganalisa kinerja jaringannya. Wireshark mampu menangkap paket-paket data atau informasi yang berjalan dalam jaringan yang terlihat dan semua jenis informasi ini dapat dengan mudah dianalisa yaitu dengan memakai sniffing , dengan sniffing diperoleh informasi penting seperti password email account lain. Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang amat berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan. Berikut ini merupakan fungsi-fungsi dari wireshark.

1. Menganalisa jaringan.
2. Menangkap paket data atau informasi yang berkeliaran dalam jaringan yang terlihat.
3. Penganalisaan informasi yang didapat dengan melakukan sniffing.
4. Membaca data secara langsung dari Ethernet, Token-Ring, FDDI, Serial (PPP dan SLIP), 802.11 wireless LAN, dan koneksi ATM.
5. Menganalisa transmisi paket data dalam jaringan, proses koneksi dan transmisi data antar komputer.
6. **Visualisasi Wireshark**

Visualisasi wireshark ini di ambil dari sebuah file capturing data selama satu menit pada web browsing dan live streaming. Dimana yang diakses pada web browsing adalah [www.gaptex.com](http://www.gaptex.com) dan pada live streaming adalah [www.vidio.com](http://www.vidio.com).

Berikut ini merupakan hasil dari visualisasi pada pcap web browsing [www.gaptex.com](http://www.gaptex.com) :











Berikut ini merupakan hasil dari visualisasi pada pcap live streaming [www.vidio.com](http://www.vidio.com) :











**BAB II**

**PENUTUP**

1. **Kesimpulan**

Wireshark adalah penganalisa paket bebas dan open source sehingga dapat digunakan dipakai oleh network administrator untuk menganalisa kinerja jaringannya. Wireshark juga mampu menangkap paket-paket data atau informasi yang berjalan dalam jaringan yang terlihat dan dapat dengan mudah untuk dianalis dan divisualisasikan.

**REFERENSI**

Eko, Yudhi. 2012. “Analisa Jaringan Menggunakan Wireshark”. (online) <http://yudy-s.blogspot.co.id/2012/03/analisa-jaringan-menggunakan-wireshark.html>. Diakses pada tanggan 5 September 2017.

Khoirani, Rahmi. 2017. “Capturing Data Menggunakan Wireshark dan CMD. (online) <http://edocs.ilkom.unsri.ac.id/id/eprint/1456>. Diakses pada tanggal 5 September 2017.

Phyong, Fiya. 2010. “Wireshark, Fungsi dan Kegunaannya”. (online) <http://fiyaphyong.blogspot.co.id/2010/10/wireshark-fungsi-dan-kegunaanya.html>. Diakses pada tanggal 5 September 2017.

Yayat. 2013. “Cara Menangkap Paket dengan Wireshark”. (online) <http://yayat-tekno.blogspot.co.id/2013/04/cara-menangkap-paket-dengan-wireshark.html>. Diakses pada tanggal 5 September 2017.