

# **SISTEM MONITORING JARINGAN WIFI MENGGUNAKAN WIRESHARK PADA STMIK KNI KRISTEN NEUMANN INDONESIA**

<sup>1</sup>Bersama Sinuraya dan <sup>2</sup>Heryco Bremana P Tarigan

**STMIK Kristen Neumann Indonesia**

Jl.Letjen Jamin Ginting KM 10.5 Medan

<sup>1</sup> [bersamaraya@gmail.com](mailto:bersamaraya@gmail.com)

<sup>2</sup> [heryco.tarigan@yahoo.co.id](mailto:heryco.tarigan@yahoo.co.id)

## ***ABSTRAK***

*STMIK Neumann ialah merupakan salah satu perguruan tinggi yang didirikan oleh YPK-GBKP. dimana pada kampus STMIK Neumann sudah memiliki jaringan WIFI meskipun jaringan WIFI tersebut belum terkoneksi ke seluruh ruangan. Dimana untuk memudahkan kita dalam memonitoring jaringan WIFI tersebut kita menggunakan Wireshark, maka tugas akhir ini di analisis dan dimonitoring dari jaringan yang sedang berjalan dengan menggunakan Wireshark, dimana jika jaringan tersebut terkoneksi dalam kampus STMIK Neumann dengan harapan bila menggunakan wireshark memudahkan kita dalam memonitoring jaringan WIFI yang menangkap semua jenis jaringan yang sedang berjalan atau yang sedang terkoneksi dengan jaringan kampus STMIK Neumann.*

*Kata Kunci: STMIK-KNI, memonitoring jaringan WIFI, WIRESHARK*

## ***Abstract***

*STMIK Neumann is one college that was founded by YPK-GBKP. Where on campus STMIK Neumann already have WIFI, WIFI network even though the network is not connected to the rest of the room. Wireshark is being used to monitor WIFI in order to capture the packet and the frames in the STMIK Neumann WIFI. Where to help us in monitoring the WIFI network we are using Wireshark, then this final task in the analysis and monitored from a network that is running by using Wireshark, where in if the network is connected in a campus STMIK Neumann with expectations when using wireshark help us in monitoring the WIFI network which captures all kinds of networks that are running or are being connected to the campus network STMIK Neumann.*

*Keywords: STMIK-KNI, WIFI network monitoring, WIRESHARK*

## 1. Pendahuluan

Wireshark merupakan aplikasi perangkat lunak (*software*) yang digunakan untuk melihat dan menganalisa paket-paket data yang lewat pada jaringan kita. Sangat mudah dipakai karena menggunakan wireshark. Semakin berkembangnya teknologi informasi sekarang ini, maka kebutuhan akan informasi semakin meningkat pula, dimana setiap orang membutuhkan informasi dalam waktu yang cepat, singkat dan akurat oleh karena itu dibutuhkan suatu sarana yang mendukung hal tersebut.

Monitoring jaringan biasanya dipakai untuk keamanan jaringan oleh suatu instansi, proses monitoring jaringan merupakan suatu cara untuk proteksi di jaringan kita. Dalam monitoring jaringan kita dapat memakai software seperti wireshark. Untuk mengaplikasikan software ini kita harus terhubung dalam suatu jaringan internet. Bila jaringan yang tidak berkinerja baik dan banyak mengalami masalah yang memerlukan pemecahan masalah, pendekatan yang lebih baik mungkin untuk upaya optimalisasi kinerja mereka dan operasi, bukan hanya pemecahan masalah untuk menyelesaikan masalah saat ini. Dengan kata lain, perusahaan ini mungkin perlu untuk mengambil dan melihat pendekatan terhadap masalah jaringan. bukan hanya mengisolasi masalah, mungkin lebih baik untuk memeriksa seluruh jaringan internet tersebut dengan menggunakan protocol analyzer atau alat pemantauan untuk mengoptimalkan kinerja jaringan, tetapi jaringan internet sering kali lambat karena adanya sebagian dari pengguna mengambil data dan terkadang kapasitas jaringan dengan sipemakai sering kali tidak sesuai.

Aplikasi ini menggunakan sistem capture, maksudnya kita dapat menentukan apa-apa saja yang kita butuhkan dalam memonitoring jaringan. Semua proses yang terjadi akan tercapture secara langsung, sehingga dari situ hanya perlu melanjutkan dengan cara memonitoring jaringan dengan wireshark. Dengan menggunakan software ini kita bisa mengcapture packet data yang berkeliaran pada jaringan yang sedang dimonitoring.

## 1.2 Rumusan Masalah

Adapun permasalahan yang muncul pada jaringan tersebut yaitu:

1. Bagaimana meningkatkan keamanan suatu jaringan menggunakan wireshark.
2. Bagaimana cara kerja wireshark.

3. Bagaimana memonitor data yang diperoleh dari layanan yang menggunakan wireshark.

## 1.3 Ruang Lingkup Pembahasan

Dalam perancangan dan implementasi system ini, terdapat masalah yang meliputi:

1. Menggunakan wireshark sebagai *Network Analyzer*.
2. Untuk memonitoring jaringan tersebut maka kita harus terhubung dengan jaringan WIFI di STMIK-KNI.

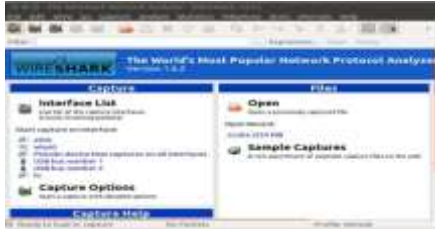
Wireshark merupakan sebuah program analisa paket jaringan yang akan menangkap paket jaringan dan mencoba untuk menampilkan data dari sebuah paket yang sedetail mungkin. Kita bisa melogikakan atau memikirkan sebuah packet *analyzer* jaringan sebagai alat ukur yang digunakan untuk memeriksa apa yang terjadi di dalam kabel jaringan. Wireshark merupakan salah satu aplikasi terbaik paket open source yang tersedia saat ini.

Beberapa tujuan penggunaan wireshark, sebagai berikut:

- a. Administrator jaringan menggunakannya untuk memecahkan masalah jaringan
- b. Insinyur keamanan jaringan menggunakannya untuk memeriksa masalah keamanan
- c. pengembang menggunakannya untuk men-debug implementasi protocol
- d. beberapa orang yang menggunakannya untuk mempelajari protokol jaringan internal

Beberapa fitur yang terdapat pada wireshark, yaitu:

- a. Capture paket data langsung dari antarmuka jaringan.
- b. Menampilkan paket dengan informasi protokol yang sangat rinci.
- c. Buka dan Simpan data paket yang diambil.
- d. Impor dan Ekspor paket data dari dan ke banyak program capture lainnya.
- e. Menyaring paket pada banyak kriteria.
- f. Pencarian untuk paket pada banyak kriteria.



Gambar 3.1 Hasil Dari Wireshark Network

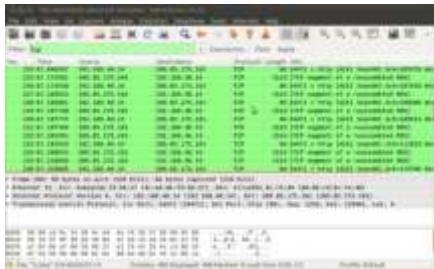
## 2. Colorize menampilkan paket berdasarkan Dari filter.



Gambar 3.2 Hasil Dari Capture Interfaces

Langkah-langkah untuk proses pengerjaan dalam dalam Capture Interfaces, sebagai berikut:

1. Pilih tabel Capture lalu di klik tombol tersebut
2. Pilih jaringan yang akan di analisis
3. Pilih tabel Start lalu di klik untuk memulai
4. Pilih tabel Stop lalu di klik Stop untuk berhenti



Gambar 3.3 Lalu lintas jaringan yang terekam pada koneksi WIFI

Penjelasan masalah jaringan WIFI yang terekam pada Wireshark, yaitu sebagai berikut:

1. Source merupakan IP Address sumber
2. Destination merupakan IP Address tujuan
3. Protocol merupakan suatu paket system yang mengatur komunikasi – komunikasi antara satu komputer ke komputer lain dalam suatu jaringan

Bagian-bagian pada wireshark sebagai berikut:

1. Packet List Pane menampilkan ringkasan dari paket-paket yang telah tertangkap oleh Wireshark.
2. Packet Detail Pane menampilkan detail dari paket yang dipilih pada Packet List Pane.
3. Packet Byte Pane menunjukkan isi data dari sebuah paket dalam heksa desimal serta menunjukkan detail dari field yang dipilih pada Packet Detail Pane.

Salah satu cara yang bisa dilakukan switch adalah melakukan proses port mirroring dari switch tersebut ke salah satu port di mana kita memasang software sniffer kita. Cuma saja, biasanya hanya product switch adalah yang manage-able yang bisa melakukan sebuah hal ini. Jika switch kita memakai unmanaged, maka prosesnya akan lebih rumit.

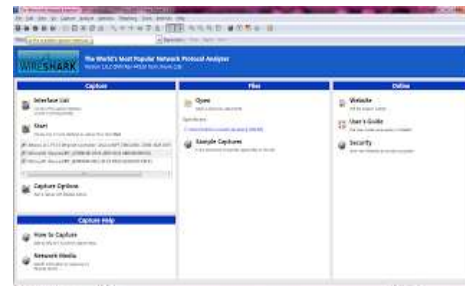


Gambar 3.4 Hasil Dari Network Administrator

Gambar di atas dapat dijadikan contoh kebanyakan jaringan yang ada dimana network administrator menginginkan memonitor jaringan ke internet. Maka yang dilakukan adalah melakukan 'port mirroring' pada link yang merah, dengan target mirror port adalah port tempat di mana wireshark dipasang. Tetapi, tentu saja untuk melakukan hal tersebut, untuk network yang berada di administrator harus mengkonfigurasi switch.

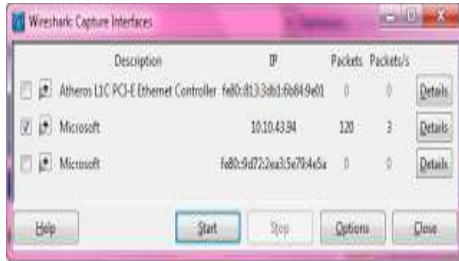
## 3. Mengetahui Situs-situs yang diakses dalam wireshark

1. Buka program Wiewshark pada Laptop atau PC anda.



Gambar 3.5 Tampilan Wiewshar

2. Buka situs apa saja untuk mencoba sebagai contoh buka [www.google.com](http://www.google.com), lalu aktifkan capture pada Wireshark dengan mengklik Capture --> interface --> pilih interface yang telah terkoneksi ke jaringan --> klik Start.



Gambar 3.6 Wireshark Saat Capture Jaringan

4. Paket-paket data dari situs yang telah diakses tadi akan tercapture



Gambar 3.7 Hasil Paket-paket Yang Dimonitoring

4. Pilih dari paket-paket yang mengirimkan pesan GET. lalu lihat paketnya, maka akan terlihat situs apa yang sedang diakses.



Gambar3.8 Wireshark Menampilkan Hasil Yang Di Monitoring

Wireshark merupakan salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya yang termasuk protokol didalamnya. Wireshark yang banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis.

Wireshark mampu menangkap paket-paket data atau informasi yang berada dalam sebuah 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 spt password email atau account lain) dengan menangkap paket-paket yang berseliweran di dalam jaringan dan menganalisanya.

Wireshark ialah merupakan sebuah software untuk melakukan sebuah analisa lalu-lintas didalam jaringan komputer, yang memiliki fungsi-fungsi yang amat berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan.

## 5. Langkah Wireshark Berjalan

Disini saya mencoba menggunakan wireshark untuk memantau akses browser yang saya jalankan. Namun disini saya mencoba memonitor jaringan wi-fi. langkah pertama untuk memilih driver wireless, saat ditampilkan awal kita bisa menekan tombol **Ctrl +K**



Gambar 4.1 List driver

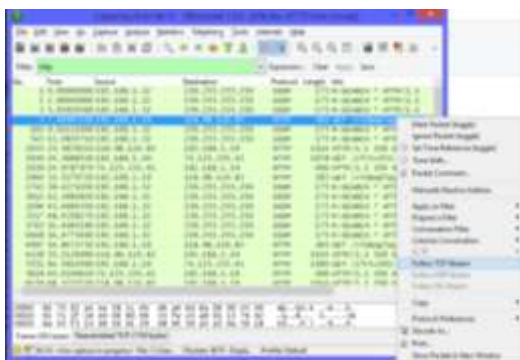
Setelah menekan Tombol Strat, maka WireShark akan langsung menampilkan packet packet data yang masuk. Untuk mempermudah monitoring gunakan sebuah filter *http*. Filter *http* ini dimaksudkan untuk menampilkan packet data yang berbasis HTTP. Dari hasil yang saya peroleh (yang saya Block) menunjukkan bahwa ada paket yang diterima dari youtube.kebetulan saat itu saya sedang streaming video di you tube.



Gambar 4.2 Hasil Paket Data dengan Filter HTTP

Dimana dari gambar 4.2 menampilkan IP pengguna jaringan dan sebuah website yang sedang diakses oleh pengguna jaringan WIFI tersebut.

Namun dari sebuah data diatas belum bisa menunjukkan hasil jumlah packet data, alamat web yang sedang dibuka maka dari itu packet yang telah dipilih tersebut kita bisa menekan tombol kanan, pilih *follow TCP stream*.



Gambar 4.3 Follow TCP Stream

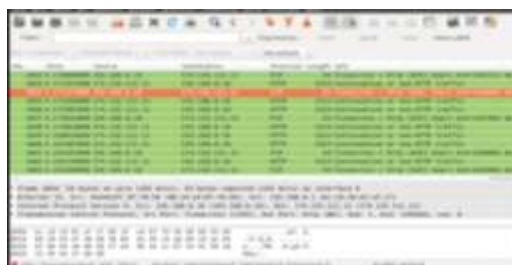
Dimana pada gambar 4.3 pada Follow TCP Stream menampilkan waktu pemakaian, IP pengguna jaringan, menampilkan wibsed yang sedang di bukak oleh pengguna jaringan WIFI tersebut.

Seperti Gambar 12. Bahwa alamat you tube yang sedang saya streaming dan telah tertangkap pada wireshark. Jadi dengan wireshark ini kita bisa memantau alamat alamat web yang kita kunjungi. Namun Video yang sedang saya tonton di youtube saat itu sudah saya play sebelum saya mengaktifkan WireShark. Dengan menggunakan Kata lain untuk jaringan Wireless, Kemampuan Wireshark ini agak berkurang yaitu WireShark hanya menampilkan data Cookie yang lama sedangkan untuk menampilkan data cookie yang baru dibutuhkan waktu yang cukup lama.



Gambar 4.4 Hasil dari Follow TCP Stream

TCP Stream ialah dimana sebuah tampilan hasil dari paket wireshark itu sendiri yang menampilkan hasil dari follow TCP Stream tersebut.



Gambar 4.5 Hasil nampil program berjalan

Dimana hasil diatas adalah sebuah program atau hasil berjalan dari paket WIRESHARK tersebut dengan menampilkan semua paket program berjalan.

## 5.1 Kesimpulan

Berdasarkan monitoring dan pembahasan pada penelitian ini, maka didapat kesimpulan sebagai berikut:

1. Untuk memonitoring jaringan WIFI, wireshark dapat berada di tempatkan untuk memonitoring jaringan.
2. Wireshark adalah sebagai bentuk dari protocol analizer data-data informasi tentang pengguna jaringan WI-FI. Dimana data-data tersebut dapat IP Adress, portnya dan alamat situsnya.

## 5.2 Saran

Adapun saran yang dapat penulis berikan kepada kampus STMIK-KNI sebagai berikut:

1. Untuk dari seluruh gedung STMIK-KNI supaya dapat di akses dengan WIFI lebih terjangkau dari seluruh titik dalam gedung tersebut.
2. Daya jangkau perangkat jaringan WIFI perlu di naikkan. Supaya jarak jangkau semakin luas.
3. Tidak terputusnya jaringan dari jaringan WIFI saat mengakses situs yang di butuhkan pada pengguna.

## Referensi

- Riyanto.B, (2006), *Perancangan Aplikasi M-Learning Berbasis Java*.Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia 3-4 Mei 2006.386-392.
- Sanders Chris. 2007. *Practical Packet Analysis Using Wireshark To Solve Real-World Network Problems*. San Fransisco: William Pollock
- Prasad Anand, Prasad Neeli. 2005. *802.11 WLANs and IP Networking Security, QoS, and Mobility*. London: Artech House
- ITU-T Y.1541., *Internet protocol aspects – Quality of service and network performance*. Februari 2006
- Orebaugh Angela, Ramirez Gilbert, Burke Josh. 2007. *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. United States: O'Reilly Media, Inc. Prasad