IMPLEMENTASI JARINGAN VPN L2TP / IPSEC MENGGUNAKAN *LINUX* DI LABORATURIUM JARINGAN KOMPUTER

Jihan Safira[1], Hanafi[2], Munawar[3]

[1,2,3]Prodi Teknologi Rekayasa Jaringan Telekomunikasi
Jurusan Teknik Elektro,Politeknik Negeri Lhokseumawe
e-mail:piehio9966@gmail.com

***Abstrak*— VPN merupakan salah satu teknik keamanan jaringan yang berguna dalam menjaga paket data dengan cara mengenkripsian suatu jaringan agar jaringan tersebut aman dari ganguan pihak luar. Penelitian tentang analisis keamanan jaringan dan kualitas jaringan menggunakan *linux debian* di lakukan di laboratorium jaringan komputer dimana hasil dari penelitian ini berupa *throughput, delay, paket loss* dan *paket sniffer*. Penelitian dilakukan dengan menggunakan metode L2TP/IPSec pada jaringan yang akan dibangun yaitu VPN dan data yang akan dikirimkan sebesar 10,20, dan 30 MB. Pada hasil rata – rata dari *throughput* ialah 3,915 Mbit / sec, 4,542 Mbit / sec, dan 5,165 Mbit / sec dimana semakin besar data yang dikirimkan semakin besar *throughput* yang dihasilkan, dengan demikian dapat dimasukan dalam TIPHON 2.1 berkualitas bagus dan sedang. Pada hasil rata – rata dari *Delay* ialah 4,186 ms, 3,791 ms, dan 1,687 ms dimana semakin sering mengirimkan data yang sama semakin sedikit waktu yang dibutuhkan untuk mengirim paket – paket data, dengan demikian dapat dimasukan dalan TIPHON 2.2 berkualitas sedang dan bagus. Pada hasil rata – rata dari paket loss ialah 0,102 %, 0,158 %, dan 0,140 % dimana pada dasarnya paket – paket yang loss apabila data yang dikirikan terlalu besar memiliki loss yang besar, dengan demikian dapat dimasukan dalan TIPHON 2.3 berkualitas sangat bagus. Pada pengujian keamanan jaringan VPN yang dibuat telah terenkripsi sehingga pada PC lainya tidak dapat melihat alur saat pengiriman data berlangsung dan pada pengujian pencurian paket data IP 192.168.12.254 tidak terdeteksi karena telah terenkripsi oleh VPN L2TP / IPSec.**

***Kata Kunci*— VPN, L2TP/IPSec, IP, Linux Debian.**

I. PENDAHULUAN

VPN menggunakan jalur akses internet yang berguna untuk mengirim atau menerima paket data yang sudah terenkripsi pada IP *Private*. Pada dasarnya internet menggunakan IP *Public* sehingga memungkinkan banyak pengguna internet menerobos masuk untuk pencurian paket data. Dengan adanya VPN seluruh paket data yang ingin dikirim dan diterima akan terenkripsi dua kali lebih aman.

VPN merupakan salah satu teknik keamanan jaringan yang berguna dalam menjaga paket data dengan cara mengenkripsian suatu jaringan agar jaringan tersebut aman dari ganguan pihak luar. VPN juga berfungsi sebagai jalur akses keamanan tambahan yang terhubung ke jaringan *Public* dengan mengengkripsi IP *Private* yang sudah ditentukan.

II. TINJAUAN PUSTAKA

A. VPN (Virtual Private Network)

VPN adalah sebuah koneksi Virtual yang bersifat *private*, mengapa disebut virtual karena pada dasarnya jaringan ini tidak ada secara fisik hanya berupa jaringan virtual dan mengapa disebut private karena jaringan ini merupakan jaringan yang sifatnya private yang tidak semua orang bisa mengaksesnya. VPN Menghubungkan PC dengan jaringan publik atau internet namun sifatnya private, karena bersifat private maka tidak semua orang bisa terkoneksi ke jaringan ini dan mengaksesnya. Oleh karena itu diperlukan keamanan data.[1]

VPN adalah singkatan dari Virtual Private Network, yaitu sebuah terowongan Virtual (*Virtual Tunnel*) dari jaringan ke jaringan lain yang terenkripsi. VPN server dan VPN Client harus saling ter-autentikasi. VPN mengkoneksikan dua jaringan seperti kantor - kantor cabang atau Remote User tunggal ke kantor. L2TP merupakan tunneling protokol pengembangan dari PPTP dari *Microsoft* dan L2F dari *Cisco*, sedangkan IPSec merupakan protokol standar kemanan dari IP.[2]

B. L2TP / IPSec

L2TP merupakan pengembangan dari PPTP ditambah L2F. dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan UDP port 1701. Biasanya untuk keamaanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec.[2]

Untuk dapat memenuhi keamanan jaringan pada VPN L2TP, maka harus disertai dengan mengimplementasikan keamanan dengan menggunakan IPSec yang disebut sebagai IP *Security*. Pada IPSec ini paket data yang dikirimkan oleh VPN L2TP dapat lebih terenkapsulasi sehingga komunikasi yang terjadi antara *Server* dan *Client* lebih aman. Terdapat perlindungan ganda pada keamanan jaringan deengan perlindungan pertama menetapkan koneksi *Point-To-Point Protocol* (PPP) antara pengirim, sedangkan perlidungan kedua merupakan enkripsi untuk keamanan yang dimiliki oleh keunggulan IPsec.

C. Linux Debian

Debian adalah sistem operasi komputer yang tersusun dari paket-paket perangkat lunak yang dirilis sebagai perangkat lunak bebas dan terbuka dengan lisensi mayoritas GNU General Public License dan lisensi perangkat lunak bebas lainnya. Debian GNU/Linux memuat perkakas sistem operasi GNU dan kernel Linux merupakan distribusi Linux yang populer dan berpengaruh. Debian didistribusikan dengan akses ke repositori dengan ribuan paket perangkat lunak yang siap untuk instalasi dan digunakan.

D. Sniffing

Sniffing merupakan proses pengendusan paket data pada sistem jaringan komputer, yang diantaranya dapat memonitor dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket itu di kirimkan. Contoh dampak negatif sniffing, seseorang dapat melihat paket data informasi seperti username dan password yang lewat pada jaringan komputer. Contoh dampak positif sniffing. Seorang admin dapat menganalisa paket-paket data yang lewat pada jaringan untuk keperluan optimasi jaringan, seperti dengan melakukan penganalisaan paket data, dapat diketahui dapat membahayakan performa jaringan atau tidak, dan dapat mengetahui adanya penyusup atau tidak.[3]

E. Pengujian Kualitas Jaringan

Throughput

Kinerja throughput adalah sebuah pengujian yang dapat mengetahui jumlah bit yang berhasil dikirim. Perhitungan throughput dengan mengetahui jumlah data yang dikirim dibagi dengan waktu pengiriman data.

$$\text{Throughput} = \frac{jumlah\ data\ yang\ dikirim}{waktu\ prngiriman\ data} \quad (1)$$

Tabel. 1 Peforma Jaringan Berdasarkan *Throughput* Standarisasi Tiphon

Throughput (Mbit / sec)	Kualitas
7,5-10,0	Sangat Bagus
5,0-7,5	Bagus
2,5-5,0	Sedang
<2,5	Jelek

Delay

Kinerja *Delay* yang paling sering dialami oleh trafik yang lewat dari pengirim dan penerima adalah *Delay* transmisi. Dengan *Delay* yang merupakan total waktu yang dibutukan paket untuk menempuh jarak asal ke tujuan. Dapat dirumuskan dalam persamaan berikut ini :

$$Delay = \frac{between\ frist\ and\ last\ packet}{packets} \quad (2)$$

Tabel. 2 Peforma Jaringan Berdasarkan *Delay* Standarisasi Tiphon

Delay (ms)	Kualitas
<1,50	Sangat Bagus
1,50-3,00	Bagus
3,00-4,50	Sedang
<4,50	Jelek

Path Loss

Kinerja *Path Loss* digunakan dalan komunikasi nirkabel. *Path Loss* disebut juga dengan banyak nya paket yang hilang disebabkan oleh tabrakan (*collision*), kelebihan kapasitas jaringan, penurunan paket yang disebabkan olehhebisnya TTL (*Time To Live*).

$$Path\ Loss = \frac{paket\ total\ tercapture - paket\ terkirim}{paket\ total\ tercapture} x\ 100\% \quad (3)$$

Tabel. 3 Peforma Jaringan Berdasarkan *Path Loss* Standarisasi Tiphon

Path loss (%)	Kualitas
0,01 – 0,30	Sangat Bagus
0,30 – 1,50	Bagus
1,50 – 2,50	Sedang
>2,50	Jelek

F. Pengujian Keamanan Jaringan

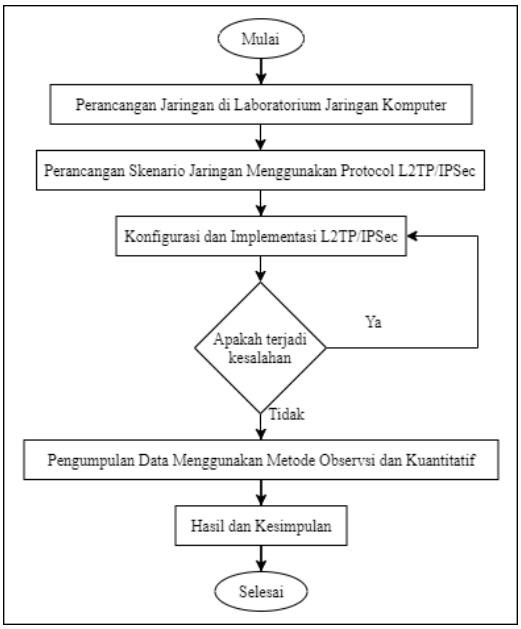
Pengujian keamanan jaringan menggunakan *Packet Sniffer* dapat terbagi menjadi dua fungsi yaitu, mengecek terenkripsi atau tidak terenkripsi sebuah VPN, dan mengecek pencurian paket data. Fungsi pertama untuk mengecek terenkripsi atau tidak dapat dilihat dengan mengkoneksi pada jaringan client yang sama setelahnya dapat mengeping pada ip public dan ip private. Sedangkan fungsi yang kedua untuk mengecek pencurian paket data dilihat dengan menerobos laju lintasan saat pengiriman data dilakukan menggunakan aplikasi *wireshark* dimana data yang dikirim harus benar – benar terenkripsi sehingga tidak dapat dilihat pada tcp *wireshark*.

III. METODOLOGI PENELITIAN

A. Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini menggunakan metode observasi dan metode kuantitatif. Metode observasi merupakan pengamatan secara langsung memlalui *WireShark* untuk melihat pemecahan masalah jaringan dan dapat melihat secara sistemetis. Sedangkan metode kuantitatif merupakan metode perhitungan sistematis untuk menghitung *Throughput, Delay* dan *packet loss.*

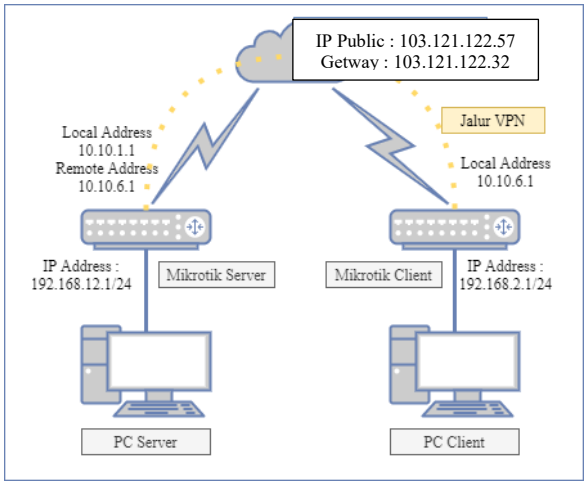
Untuk dapat lebih jelas alur dari teknik pengumpulan data dapat dilihat pada *Flowchart* berikut ini.



Gambar. 1 Flowchart Penelitian

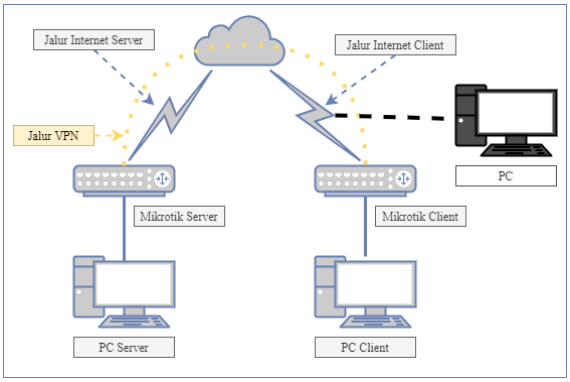
B. Perancangan Mikrotik

Perancangan mikrotik memiliki remote address dan local address yaitu, local address adalah alamat IP yang akan terpasang pada router server sedangkan remote address adalah alamat IP yang akan diberikan kepada client.



Gambar. 2 Perancangan Mikrotik dari Server ke Client

Pada mikrotik server dengan ip 192.168.12.1/24 memiliki local address dengan ip 10.10.1.1 dan remote address degan ip 10.10.6.1 yang melalui internet dengan ip public 103.121.122.57 yang terhubung ke sisi client.



Gambar. 3 Skenario Serangan

Skenario serangan mikrotik dapat dijelaskan bahwasanya dari PC server terhubung ke mikrotik sever. Untuk menguji terenkripsinya sebuah VPN penulis menambahkan serangan pada bagian client dengan *Opersi System Windows* XP. Pada saat server mengirimkan paket data ke sisi client dapat dilihat dengan mengunakan tcp *Wireshrak* dengan ip 192.168.12.254, ip yang dimaksud adalah ip FTP.

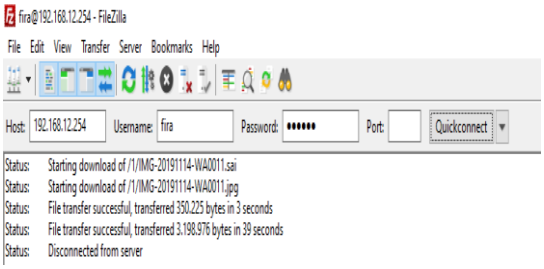
C. Metode Analisis Data

Metode analisis yang digunakan adalah metode observasi dan metode kuantitaif. Metode obervasi merupakan pengamatan secara langsung ke objek penelitian seperti pada parameter keamanan jaringan yang menggunakan aplikasi *Wireshark* yang dapat mendeteksi adanya terenkripsi atau tidak terenkripsi dan melihat adanya pencurian paket data dengan *Packet Sniffer*. Sedangkan metode kuantitatif merupakan perhitungan berdasarkan kualitas jaringan seperti *Throughput, Delay,* dan *Path Loss.*

IV. HASIL DAN PEMBAHASAN

A. *Server* VPN

VPN server dengan metode L2TP / IPSec dapat dibangun dengan ketentuan yang sudah ditentukan agar terkoneksi ke PC. Untuk dapat tehubung pada sisi client VPN server harus memiliki username, password berserta port untuk dapat terkoneksi secara private untuk itu dapat dilihat pada gambar 4 berikut ini:



Gambar. 4 *Username, Password* Dan Port

B. Pengujian Kualitas Jaringan

1. Throughput

Hasil pengujian dapat dilihat pada tabel 4 dibawah ini.

Tabel. 4 Hasil Pengujian *Throughput*

Besar Data Yang Di Transfer	Througput (Mbit / sec)					
	Uji1	Uji2	Uji3	Uji4	Uji5	Rata - Rata
10 MB	7,701	3,440	3,374	3,250	1,811	3,915
20 MB	1,288	7,014	5,565	4,408	4,436	4,542
30 MB	5,344	4,743	4,885	5,331	5,320	5,165

Hasil rata – rata dari *Throughput* pada pengujian paket data yang dikirimkan sabesar 10, 20, dan 30 MB dapat dimasukan dalam tabel TIPHON. Dimana rata – rata dari *Throughput* 10 MB adalah 3,915 Mbit / sec termasuk kualitas **sedang**. Sedangkan pada rata – rata *Throughput* 20 MB adalah 4,542 Mbit / sec termasuk kualitas **sedang**. Kemudian pada rata–rata *Throughput* 30 MB adalah 5,165 termasuk kualitas **bagus**

2. *Delay*

Pada pengujian paket data yang dikirimkan sebesar 10, 20, dan 30 MB diperoleh nilai rata-rata dari *Delay* 10 MB adalah 4,186 ms termasuk kualitas **sedang**. Sedangkan pada rata – rata *Delay* 20 MB adalah 3,791 ms termasuk kualitas **sedang**. Kemudian pada rata – rata *Delay* 30 MB adalah 1,687 ms termasuk kualitas **bagus**.Hasil pengujian dapat dilihat pada Tabel 5.

Tabel. 5 Hasil Pengujian *Delay*

Besar Data Yang Di Transfer	*Delay* (ms)					
	Uji1	Uji2	Uji3	Uji4	Uji5	Rata - Rata
10 MB	1,124	2,509	2,509	2,291	4,257	4,186
20 MB	0,891	1,299	1,609	1,8884	1,867	3,791
30 MB	1,699	1,734	1,591	1,703	1,703	1,687

3. *Path Loss*

Dari hasil pengujian pada tabel 6, maka diperoleh rata – rata dari paket loss pada pengujian paket data yang dikirimkan sabesar 10, 20, dan 30 MB dapat dibandingkan dengan standar TIPHON. Dimana rata – rata dari paket loss 10 MB adalah 0,102 % termasuk kualitas **sangat bagus**. Sedangkan pada rata – rata paket loss 20 MB adalah 0,158 % termasuk kualitas **sangat bagus**. Kemudian pada rata–rata paket loss 30 MB adalah 0,140 % termasuk kualitas **sangat bagus**.

Tabel. 6 Hasil Pengujian *Path Loss*

Besar Data Yang Di Transfer	Paket loss (%)					
	Uji1	Uji2	Uji3	Uji4	Uji5	Rata - Rata
10 MB	0,13	0,09	0.09	0,09	0,20	0,102
20 MB	0,05	0,05	0,06	0,33	0,30	0,158
30 MB	0,07	0,26	0,25	0,06	0,06	0,140

Apabila saat melakukan ping di jaringan yang sama dengan client terdapat hasil yang memungkinkan ip private terbuka maka VPN yang dibuat tidak terenkripsi secara menyeluruh, akibatnya banyak kebocoran data yang terjadi. Sedangkan apabila ip VPN tidak dapat terlihat pada serangan PC lainya maka terenkripsi secara menyeluruh.

Kemudian dibawah ini adalah hasil dari ping IP pada mikrotik yaitu IP server 192.168.12.1 dan IP client 192.168.2.1 dapat dilihat bahwasanya pada saat PC lainya mengeping IP tersebut tidak dapat terdeteksi karena telah terenkripsi oleh IP VPN pada remote address dan local address yang telah dibuat.

```
C:\Users\Ihsan>ping 192.168.12.1

Pinging 192.168.12.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.12.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Gambar. 5 Hasil Ping PC Lainya ke IP *Server*

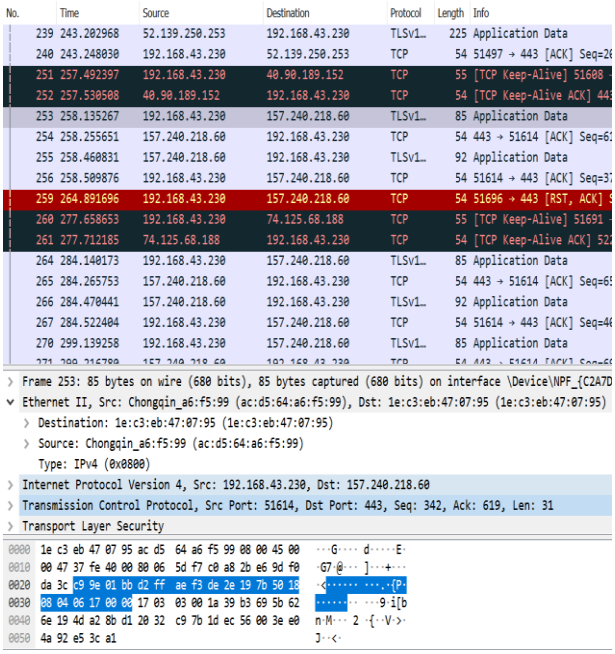
```
C:\Users\Ihsan>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.129.17: Destination net unreachable.
Reply from 192.168.129.17: Destination net unreachable.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
```

Gambar. 6 Hasil Ping PC Lainya ke IP *Client*

Pengujian keamanan jaringan untuk mengecek pencurain paket data ini dapat dilihat pada aplikasi *Wireshark* dimana IP yang harus terlihat untuk dapat mengecek pencurian paket data adalah 192.168.12.254, akan tetapi IP tersebut terenkripsi oleh adanya VPN. Dimana fungsi VPN itu sendiri ialah untuk mengakses jaringan public yang didalamnya sudah memiliki IP peivate yang hanya dimiliki oleh dirinya sendiri. Oleh karena itu IP FTP 192.168.12.254 tidak dapat terlihat pada *Wireshark* dan hanya IP 192.168.43.230 yang terlihat oleh *Wireshark.*



Gambar. 7 Hasil Pegujian dari PC lainnya

Dapat terlihat bahwasaya IP FTP untuk dapat berkomunikasi antara server dan clinet tidak dapat terlihat oleh PC lainya karena IP pada FTP telah terenkripsi dengan VPN L2TP / IPSec. Maka dapat disimpulakn bahasanya VPN L2TP / IPSec sudah terenkripsi dan tidak dapat dilihat oleh orang lain.

V. KESIMPULAN

Dapat diambil beberapa kesimpulan mengenai implemetasi jaringan VPN L2TP / IPSEC menggunakan linux dari hasil penelitian, yaitu:

1. Rata – rata dari *Throughput* 10 MB adalah 3,915 Mbit / sec termasuk kualitas **sedang**. Sedangkan pada rata – rata *Throughput* 20 MB adalah 4,542 Mbit / sec termasuk kualitas **sedang**. Kemudian pada rata – rata *Throughput* 30 MB adalah 5,165 termasuk kualitas **bagus**.
2. Nilai *Delay* 10 MB adalah 4,186 ms termasuk kualitas **sedang**. Sedangkan pada rata – rata *Delay* 20 MB adalah 3,791 ms termasuk kualitas **sedang**. Kemudian pada rata – rata *Delay* 30 MB adalah 1,687 ms termasuk kualitas **bagus**.
3. Rata-rata paket loss dari data 10 MB adalah 0,102 % termasuk kualitas **sangat bagus**. Sedangkan pada rata – rata paket loss 20 MB adalah 0,158 % termasuk kualitas **sangat bagus**. Kemudian pada rata–rata paket loss 30 MB adalah 0,140 % termasuk kualitas **sangat bagus**
4. Pada pengujian keamanan jaringan untuk mengecek data terenkripsi atau tidak, dimana hasil ping yang didapatkan terdapat hanya IP public saja terlihaat oleh PC lainya maka dikatakan VPN L2TP / IPSec yang dibuat terenkripsi sehingga pihak lain tidak dapat mengakses IP tersebut.
5. Pengujian keamanan jaringan untuk mengecek pencurain paket data ini dapat terlihat pada aplikasi *Wireshark,* dimana hasil yang didapatkan hanya IP 192.168.43.230 sedangkan untuk dapat melihat jalannya pengiriman data pada IP FTP yaitu 192.168.12.254 tidak terlihat dikarekan IP tersebut berada pada IP VPN yang melewati IP public sehingga dapat berkomunikasi secara terenkripsi dan real time.

REFERENSI

[1] Pribadi , P. T. “Implementasi High-Availability VPN Client Pada Jaringan Komputer Fakultas Hukum Universitas Udayana” . *Jurnal Ilmu Komputer* - (2013). *Volume 6 - No 1* , 21.

[2] Farly, K. A., Najoan, X. B., & Lumenta , A. S. Perancangan dan Implementasi VPN Server dengan menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi . *E-Journal Teknik Informatika* (2017). *Vol 11, No.1* , 1-7.

[3] Adriant, M. F., & Mardianto, I. IMPLEMENTASI WIRESHARK UNTUK PENYADAPAN (SNIFFING) PAKET DATA JARINGAN . *Seminar Nasional Cendekiawan* , (2015). 224-225.