ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) KANTOR PEMERINTAHAN KOTA BATAM TERHADAP SERANGAN PACKET SNIFFING

SKRIPSI

Oleh:

Maulana Muhammad Ibrahim

150210191

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KOMPUTER

UNIVERSITAS PUTERA BATAM

TAHUN 2020

ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) KANTOR PEMERINTAHAN KOTA BATAM TERHADAP SERANGAN PACKET SNIFFING

SKRIPSI

Untuk memenuhi salah satu syarat

memperoleh gelar Sarjana

Oleh:

Maulana Muhammad Ibrahim

150210191

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KOMPUTER

UNIVERSITAS PUTERA BATAM

TAHUN 2020

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini saya:

Nama : Maulana Muhammad Ibrahim

NPM : 150210191

Fakultas : Teknik Dan Komputer

Program Studi : Teknik Informatika

Menyatakan bahwa “Skripsi” yang saya buat dengan judul :

ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) KANTOR PEMERINTAHAN KOTA BATAM TERHADAP SERANGAN PACKET SNIFFING.

Adalah hasil karya sendiri dan bukan “duplikasi” dari karya orang lain sepengetahuan saya, didalam naskah Skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata didalamnaskah Skripsi ini dapat dibuktikan terdapat unsur – unsur PLAGIASI, saya bersedia naskah skripsi ini digugurkan dan gelar akademik yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang – undangan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun.

Batam, 20 Februari 2020

Yang membuat pernyataan,

Maulana Muhammad Ibrahim

140810372

ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) KANTOR PEMERINTAHAN KOTA BATAM TERHADAP SERANGAN PACKET SNIFFING

SKRIPSI

Untuk memenuhi salah satu syarat

guna memperoleh gelar Sarjana

Oleh

Maulana Muhammad Ibrahim

150210191

Telah disetujui oleh Pembimbing pada tanggal

seperti tertera dibawah ini

Batam, 20 Februari 2019

Sestri Novia Rezki, S.Kom., M.Kom.

Pembimbing

ABSTRAK

Jaringan komputer memiliki dua media transmisi data, kabel dan nirkabel. Kantor Pemerintah Kota Batam adalah salah satu Kantor Pemerintah pusat di Kota Batam yang memiliki fasilitas jaringan nirkabel (wifi). Jaringan WiFi sangat rentan terhadap ancaman serangan, karena komunikasi yang terjadi terbuka. Diperlukan sistem keamanan yang baik untuk dapat menjaga keamanan data pengguna untuk menghindari serangan yang dilakukan oleh orang-orang yang tidak bertanggung jawab. Penelitian ini membahas menganalisis tingkat keamanan fasilitas wifi di Kantor Pemerintah Kota Batam menggunakan aplikasi Wireshark. Wireshark adalah alat peretasan wifi yang digunakan untuk mendeteksi dan mengidentifikasi sinyal nirkabel terbuka dan digunakan untuk menganalisis protokol jaringan dan mengaudit keamanan jaringan, yang juga memiliki kemampuan untuk memblokir lalu lintas di jaringan LAN, mencuri kata sandi, dan membuat penyadapan aktif pada protokol umum . Dalam penelitian ini dua tahap dilakukan, yang pertama mengidentifikasi keberadaan dan keamanan wifi. Tahap kedua adalah serangan paket sniffing menggunakan perangkat lunak wireshark sebagai langkah pengujian keamanan di Kantor Pemerintah Kota Batam. Hasil dari penelitian ini adalah deteksi keberadaan dan keamanan keamanan wifi terbuka atau tidak aman dan pencatatan nama pengguna dan kata sandi. Hal ini dapat membahayakan keamanan lalu lintas data pengguna jaringan wifi dan LAN kabel terutama karyawan / i, sehingga perlu meningkatkan keamanan yang baik untuk dapat mencegah / menangani serangan paket sniffing dan banyak lagi.

Kata kunci: Keamanan Jaringan, Paket Sniffing, Peretasan, Wireshark

ABSTRACT

Computer networks have two data transmission media, wired and wireless. Batam City Government Office is one of the central Government Offices in Batam City that has wireless network facilities (wifi). WiFi networks are very vulnerable to attack threats, because the communication that occurs is open. A good security system is needed to be able to maintain the security of user data to avoid attacks carried out by people who are not responsible. This study discusses analyzing the level of security of wifi facilities at the Batam City Government Office using the Wireshark application. Wireshark is a wifi hacking tool that is used to detect and identify open wireless signals and is used to analyze network protocols and audit network security, which also has the ability to block traffic on LAN networks, steal passwords, and make active eavesdropping on common protocols . In this study two stages were carried out, the first identifying the presence and security of wifi. The second stage is packet sniffing attack using wireshark software as a security testing step in Batam City Government Office. The results of this study are the detection of the existence and security of open or unsecured wifi security and the recording of a username and password. This can endanger the security of data traffic of users of wifi networks and wired LANs especially employees / i, so it is necessary to increase good security to be able to prevent / handle packet sniffing attacks and more.

Keywords: *Network Securty, Packet Sniffing, Hacking, Wireshark*

KATA PENGANTAR

Puji Syukur kepada Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Rektor Universitas Putera Batam.
2. Ketua Program Studi Teknik Informatika Universitas Putera Batam.
3. Ibu Sestri Novia Rezki, S.Kom., M.Kom., selaku pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Dosen dan Staff Universitas Putera Batam.
5. Keluarga besar penulis yang telah memberikan dukungan dan pengertian yang begitu besar kepada penulis.
6. Teman-teman seperjuangan yang juga selalu memberikan motivasi baik berupa sharing pendapat hal-hal lainnya dalam rangka pembuatan penelitian ini.
7. Kantor Pemerintah Kota Batam yang telah mengizinkan peneliti untuk melakukan penelitian di kantor tersebut.
8. Irfan Syarif HSB, S.Kom. yang bersedia memberikan arahan kepada peneliti.

9. Serta semua pihak yang tak dapat peneliti sebutkan satu persatu yang telah membantu dalam penyusunan proposal penelitian ini.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Batam, 20 Februari 2020

Maulana Muhammad Ibrahim

DAFTAR ISI

HALAMAN SAMPUL DEPAN ..... **i**
HALAMAN JUDUL ..... **ii**
SURAT PERNYATAAN ..... **iii**
HALAMAN PENGESAHAN ..... **iv**
ABSTRAK ..... **v**
ABSTRACT ..... ***vi***
KATA PENGANTAR ..... **vii**
DAFTAR ISI ..... **ix**
DAFTAR GAMBAR ..... **xi**
DAFTAR TABEL ..... **xiii**
BAB I **1**
PENDAHULUAN **1**
1.1. Latar Belakang Penelitian 1
1.2. Indentifikasi Masalah 3
1.3. Pembatasan Masalah 4
1.4. Perumusan Masalah 4
1.5. Tujuan Penelitian 4
1.6. Manfaat Penelitian 5
BAB II **6**
KAJIAN PUSTAKA **6**
2.1. Teori Dasar 6
2.2. Teori Khusus 17
2.3. Tools 19
2.4. Penelitian Terdahulu 20
2.5. Kerangka Pemikiran 24
BAB III **26**
METODE PENELITIAN **26**
3.1. Desain Penelitian 26
3.2. Analisis Jaringan Lama/ yang Sedang Berjalan 27

3.3. Rancangan Jaringan yang Dibangun/Diusulkan 29
3.4. Lokasi dan Jadwal Penelitian 30
BAB IV 32
METODE PENELITIAN 32
4.1. Hasil Penelitian 32
4.2. Pembahasan 44
BAB V 47
KESIMPULAN DAN SARAN 47
5.1. Kesimpulan 47
5.2. Saran 47
DAFTAR PUSTAKA 49
CURICULUM VITAE 50

DAFTAR GAMBAR

Gambar 2.1 LAN (*Local Area Network*) **9**
Gambar 2.2 MAN (*Metropolitan Area Network*) **9**
Gambar 2.3 WAN (*Wide Area Network*) **10**
Gambar 2.4 Internet **10**
Gambar 2.5 Model *OSI Layer* **11**
Gambar 2.6 Physical layer **12**
Gambar 2.7 Data *Link Layer* **13**
Gambar 2.8 Network Layer **14**
Gambar 2.9 Transport Layer **15**
Gambar 2.10 Session Layer **16**
Gambar 2.11 Presentation Layer **16**
Gambar 2.12 Aplication Layer **17**
Gambar 2.13 *Wireshark versi* 3.0.2 ..... **20**
Gambar 2.14 Kerangka Pemikiran **24**
Gambar 3.1 Desain Penelitian **26**
Gambar 3.2 Topologi Jaringan yang S.edang Berjalan **27**
Gambar 3.3 Topologi Jaringan yang Diusulkan **29**
Gambar 4.1. Tampilan *Setup Wizard* **33**
Gambar 4.2. Tampilan License Agreement Wireshark **33**
Gambar 4.3. Tampilan *install Component* **34**
Gambar 4.4 Tampilan *Additional Tasks* **35**
Gambar 4.5 Tampilan Choose Instal Location **35**
Gambar 4.6 Tampilan *Packet Capture* **36**
Gambar 4.7 Proses Instal Software Wireshark **36**
Gambar 4.8 Tampilan License Agreement Npcap **37**
Gambar 4.9 Tampilan *Installation Options* **37**
Gambar 4.10 Tampilan Proses instalasi *Npcap* **38**
Gambar 4.11 Instalasi *Npcap* Selesai **38**
Gambar 4.12 Instalasi *Wireshark* selesai **39**
Gambar 4.13 Tampilan *Setup Finish* **39**

Gambar 4.14. Menghubungkan jaringan *wireless* **40**
Gambar 4.15. Tampilan *Wireshark*..... **40**
Gambar 4.16 Tampilan *Capture Interface*..... **41**
Gambar 4.16 Tampilan *Website*..... **41**
Gambar 4.17 Tampilan *Monitoring*..... **42**
Gambar 4.18 Tampilan *Command Prompt*..... **43**
Gambar 4.19 Tampilan Proses *Filter*..... **43**
Gambar 4.20 Tampilan Capture Packet Sniffing..... **44**

DAFTAR TABEL

Tabel 2.1 Badan Pekerja di IEEE **8**
Tabel 3.1 Perangkat Keras yang Sedang Berjalan **28**
Tabel 3.2 Perangkat Keras yang Sedang Berjalan **30**
Tabel 3.3 Jadwal Penelitian **31**

BAB I

PENDAHULUAN

1.1. Latar Belakang Penelitian

Di era ini banyak *issue* wacana keamanan jaringan serta keamanan jaringan sangat penting buat pada perhatikan sebab suatu jaringan yang terkoneksi atau terhubung ke internet pada dasarnya tidak aman dan selalu dapat di *monitoring* oleh para *hacker*, baik jaringan *wired LAN* maupun *wireless LAN*. Saat *file* atau data yang akan dikirim melewati beberapa terminal di jaringan berarti akan memberikan kesempatan kepada pengguna lain atau *hacker* untuk menyadap atau mengubah *file* atau data tersebut. Dalam membangun perancangan jaringan, sistem keamanan jaringan yang akan menghubungkan ke internet harus direncanakan dan harus di pahami dengan sangat baik karena agar dapat melindungi sum`ber daya seperti *file* atau data yang berada dalam jaringan itu tersebut secara aman, efektif dan meninimalisir terjadinya serangan oleh para *hacker*.

Wireshark adalah *tools pakcet sniffing* yang digunakan untuk menganalisa terhadap protokol jaringan dan mengaudit keamanan jaringan. *Wireshark* juga mempunyai kemampuan untuk mem*block* lalu lintas yang lewat pada jaringan *LAN*, mencuri *password*, dan menyadap protokol-protokol umum yang aktif, dengan adanya *wireshark* maka dipastikan di selesaikan terhadap masalah yang timbul agar tidak terjadi, bisa diartikan bahwa *wireshark* merupakan aplikasi atau *software* untuk menganalisa gerak-gerik yang mencurigakan. Tetapi

banyak masyarakat yang masih belum paham menggunakan aplikasi *wireshark.*

Kantor Pemerintah Kota Batam sudah menerapkan sebuah jaringan *LAN* dan *WLAN* sebagai media *sharing* data/informasi pelayanan umum atau komersial, kepegawaian dan informasi penting lainnya. Terdapat jaringan yang terpasang pada setiap ruangannya masing-masing, *wifi* setiap ruangan ini lah yang sering rentan dari para orang yang tidak bertanggung jawab atau *hacker*. Banyak pengguna jaringan *wifi* yang tidak tau tentang jenis bahaya apa yang menghampiri mereka pada saat berasosiasi dengan *wireless access point* (WPA).

Kebutuhan terhadap jaringan personal komputer sangatlah bertambah penting dalam pekerjaan, pendidikan maupun pada permainan dan dalam mengelola sebuah keamanan jaringan personal komputer itu sendiri, menggunakan banyaknya akses masuk kedalam itu jaringan tadi maka banyak peluang oleh para *hacker* untuk kejahatan yg akan terjadi pada jaringan tersebut, misalkan adanya peretas atau mencuri data/informasi penting yang terjadi pada jaringan tadi atau pun adanya *hacker* yang sengaja mematikan sumber daya jaringan itu tersebut. (Sulaiman, 2016).

Secara teknis operasional, *wifi* merupaka bagian berasal keliru satu varian teknologi komunikasi serta informasi yang bekerja di sebuah jaringan komputer serta perangkat *WLAN (wireless local area network)* (Jamaludin, 2016).

Penggunaan jaringan *wireless* di Kantor Pemerintah Kota Batam dapat digunakan pada karyawan maupun rakyat umum. Dengan adanya jaringan internet tadi, tentu saja sangat diperlukan suatu keamanan jaringan terutama di jaringan

wireless sebab di jaringan ini bisa diakses oleh seluruh orang. Selain itu buat meningkatkan pelayanan karyawan serta masyarakat, hal-hal yang perlu di antisipasi yaitu serangan terhadap fasilitas internet pada setiap ruangan. Salah satu potensi penyerangan keamanan jaringan yaitu *packet sniffing*. *Packet sniffing* merupakan proses penyadapan atau memonitoring terhadap paket data di jaringan komputer, yang diantaranya dapat mencuri serta mengambil seluruh lalu lintas jaringan yang lewat tanpa peduli kepada siapa pemilik paket itu yang pada curi (Adriant dan Mardianto, 2015).

Banyaknya tindakan yang terjadi dalam pencurian informasi atau data karyawan seperti *username* serta *password* asal suatu akun atau data-data penting disebabkan sang *hacker* karena tidak adanya perlindungan terhadap aspek *confidentialit* pada suatu jaringan komputer (Babys, Kusrini, & Sudarmawan, 2013).

Berdasarkan penjabaran pada di atas, penulis tertarik untuk mempelajari bagaimana mengamankan suatu jaringan. Oleh karena itu, penulis mengambil bahan tentang keamanan jaringan terhadap internet buat judul skripsi "ANALISIS KEMANAN JARINGAN PADA FASILITAS (*WIFI)* DIPEMERINTAHAN KOTA BATAM TERHADAP SERANGAN PACKET SNIFFING".

1.2. Indentifikasi Masalah

Sesuai latar belakang yang telah dijelaskan di atas, maka di identifikasi masalah yang bisa disimpulkan, seperti :

1. Ada beberapa jenis serangan yang akan masuk kedalam jaringan *wireless*.

2. Jaringan komputer dengan jangkuan *wireless* bisa juga di curi oleh orang luar mengenai data yang penting.
3. Belum adanya pendeteksi serangan di Pemerintah Kota Batam.

1.3. Pembatasan Masalah

Pada pembuatan skripsi ini, penulis membatasi masalah yang akan dianalisis yaitu :

1. Menganalisa keamanan jaringan *wireless* di Kantor Pemerintah Kota Batam.
2. Melakukan pengujian terhadap keamanan jaringan di Kantor Pemerintah Kota Batam.
3. Pengujian dengan menggunakan metode aplikasi *wireshark* terhadap *packet sniffing*.

1.4. Perumusan Masalah

Berdasarkan identifikasi masalah dapat dirumuskan yaitu sebagai berikut :

1. Bagaimana cara menganalisa paket data pada jaringan *wireless* di Kantor Pemerintah Kota Batam terhadap *packet sniffing*?
2. Bagaimana mengevaluasi keamanan jaringan *wireless* di Kantor Pemerintah Kota Batam terhadap *packet sniffing*?

1.5. Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini yaitu :

1. Untuk menganalisa keamanan jaringan *wireless* di Kantor Pemerintah Kota Batam terhadap *packet sniffing.*

2. Untuk mengevaluasi keamanan jaringan *wireless* di Kantor Pemerintah Kota Batam terhadap *packet sniffing*.

1.6. Manfaat Penelitian

Penelitian ini bermanfaat untuk, antara lain :

1. Sebagai data atau informasi yang bisa diberikan dan digunakan oleh pihak IT di Kantor Pemerintah Kota Batam guna mengamankan sebuah jaringan Komputer *LAN* atau *WLAN* agar lebih aman dan baik.
2. Sebagai pengetahuan untuk karyawan atau pengguna yang menggunakan layanan/fasilitas internet (*wifi* maupun kabel *LAN*) khususnya bagi pengguna yang umum terhadap bahaya jaringan *LAN* tanpa pengamanan yang tidak ketat.

BAB II

KAJIAN PUSTAKA

2.1. Teori Dasar

Penjelasan terhadap teori yang paling tidak berisi suatu penjelasan variabel-variabel yang akan diteliti melalui penjelasan, dan uraian yang sangat lengkap serta buat mendalami berbagai acuan, sehingga cakupan, kedudukan dan prediksi terhadap suatu hubungan antara varibel yang akan diteliti sebagai lebih tepat serta jelas (Sugiyono, 2014).

Berikut ini adalah penjelasan mengenai jaringan personal komputer, standar jaringan komputer, jenis jaringan komputer, model *OSI Layer*, dan *wireshark*.

2.1.1. Jaringan Komputer

Internet ialah istilah asal internet connection networking bisa diartikan menjadi sebuah jaringan yang saling bekerjasama, semakin banyak yg muncul beberapa teknologi yg memakai internet. seluruh bisa menikmati berbagai macam fasilitas internet jikan ingin mencari sesuatu tentang informasi atau data. untuk terhubung kepengguna, pengguna harus menggunakan pelayanan atau fasilitas khusus yg biasa disebut ISP (Internet Service Provider). Jika telah terhubung ke server ISP, user sudah mampu akses ke seluruh jaringan internet. perseteruan yg seringkali timbul terhadap koneksi internet yang sering tersendat bahkan terputus, padahal menjadi pengguna menginginkan koneksi internet yg *safety* serta lancar. (Hakim, 2017)

Personal komputer jaringan internet yang membuat sebuah konsep korelasi/interkoneksi terhadap sekumpulan perangkat. Setiap perangkat yg saling terhubung, apabilan terdapat beberapa perangkat yg tidak tersamsung, maka konsep tadi bukan termasuk ke dalam definisi jaringan. (Nugroho, 2016)

Berdasarkan kutipan dari (Ardiantoro, Taufik; Triyono, Joko; Fatkhiyah, 2016), jaringan komputer merupakan beberapa komputer yang saling terhubung satu dengan yang lainnya dengan menggunakan sebuah protokol komunikasi sehingga dapat saling *sharing* data, aplikasi, perangkat keras dan informasi secara bersamaan. Tujuan membangun jaringan komputer artinya memberikan berita Bila ada kesalahan dari pengirim (transmitter) ke penerima (receiver) melalui media komunikasi.

Berdasarkan kutipan dari (Haryanto, Muhammad Dedy; Riadi, 2014) bahwa jaringan personal komputer artinya sebuah jaringan terdiri lebih asal satu personal komputer yg saling terhubungan antara satu menggunakan yg lainnya, serta saling menyebarkan sumber daya misalnya CDROM, Printer, Pertukaran arsip, atau memungkinkan buat saling berkomunikasi secara elektronika. komputer yg saling bekerjasama dimungkinkan dengan gelombang radio, satelit, infrared, media kabel, atau saluran telepon.

2.1.2. Standar Jaringan Komputer

Beberapa badan dunia yang melakukan standarisasi jaringan komputer, badan pekerja yang dibuat ole *IEEE* yang banyak membuat standarisasi buat alat-alat telekomunikasi mirip yang tertera pada tabel berikut (Maslan, 2012) :

Working Group	Bentuk Kegiatan
IEEE802.1	Standart LAN/MAN
IEEE802.2	Standart *Logical Link Control* (LLC).
IEEE802.3	Standart untuk *Ethernet Coaxial* atau UTP
IEEE802.4	Standart *Token Bus*.
IEEE802.5	Standart *Token Ring*.
IEEE802.6	Standart MAN-DQDB.
IEEE802.7	Standart LAN *Broadband*
IEEE802.8	Standart FDDI
IEEE802.9	Standart ISDN
IEEE802.10	Standart LAN/MAN untuk VPN
IEEE802.11	Standart LAN nirkabel untuk *Wifi*
IEEE802.12	Standart DPAM (*Demand Priority Access Method*)
IEEE802.15	Standart PAN nirkabel untuk IrDA dan *Bluetooth*
IEEE802.16	Standart *WiMAX*

Tabel 2.1 Badan Pekerja di IEEE

2.1.3. Jenis Jaringan Konputer

Jenis jaringan komputer bisa dibagi sesuai kriteria seperti sebagai berikut:

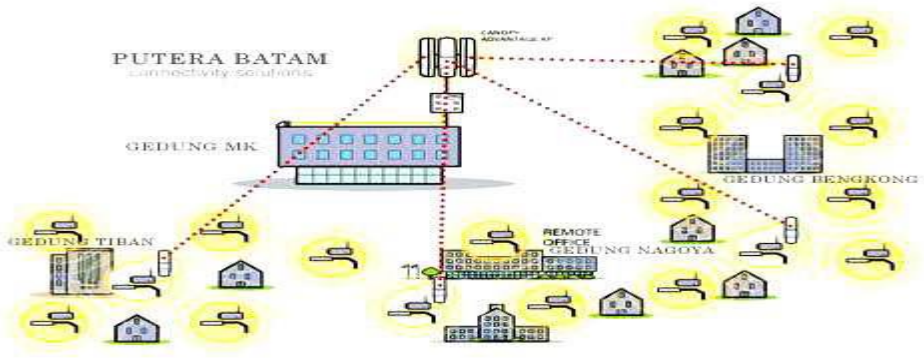
Jaringan komputer berdasarkan jangkuan dibagi menjadi 4 jenis, yaitu (Maslan, 2012) :

1. *LAN (Local Area Network)*, adalah jaringan komputer dalam ruang lingkup gedung atau kampus yang ukuran hanya beberapa kilometer.

LAN seringkali dipergunakan buat terhubung ke komputer-komputer pada kantor atau perusahaan buat pemakaian secara bersama dan saling bertukar data/info ke sesama.

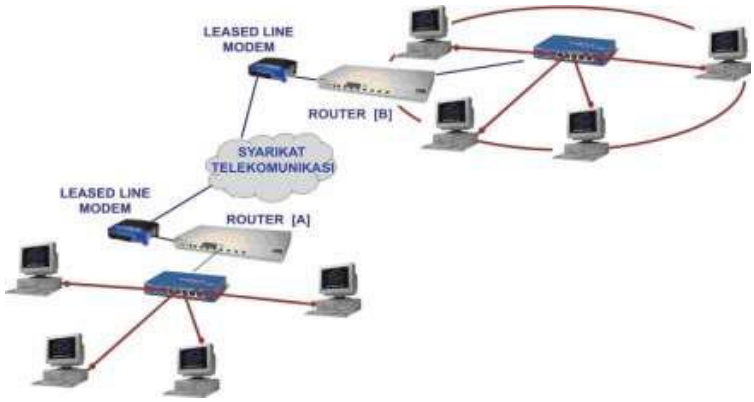
Gambar 2.1 LAN (*Local Area Network*)

2. *MAN (Metropolitan Area Network)*, adalah versi yg ukuran lebih besar berasal pada LAN, teknologi yg dipergunakan masih sama seperti menggunakan LAN. MAN yg mencakup antar beberapa perusahaan yang berdekatan atau jua sebuah kota serta bisa dimanfaatkan buat keperluan eksklusif atau awam. MAN mampu menunjang data serta bunyi bahkan bisa dipergunakan buat aplikasi TV kabel.



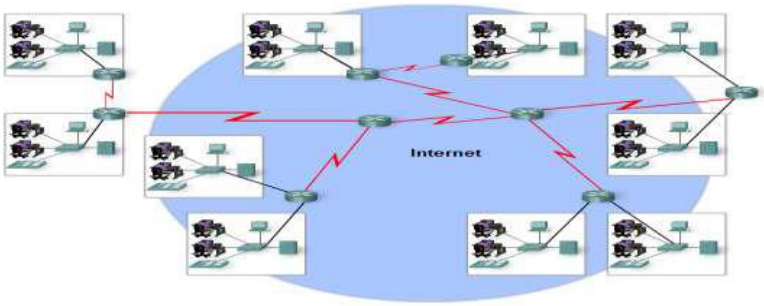
Gambar 2.2 MAN (*Metropolitan Area Network*)

3. *WAN (Wide Are Network)*, jangkauan meliputi wilayah geografis yg sangat luas, jangkauannya bisa negara bahkan benua. Teknologi yg dipergunakan hampir sama menggunakan LAN.



Gambar 2.3 WAN (*Wide Area Network*)

4. *INTERNET (Interconnected Network)*, jangkauannya meliputi seluruh global yg artinya adonan asal LAN, WAN, dan MAN yg terdapat.



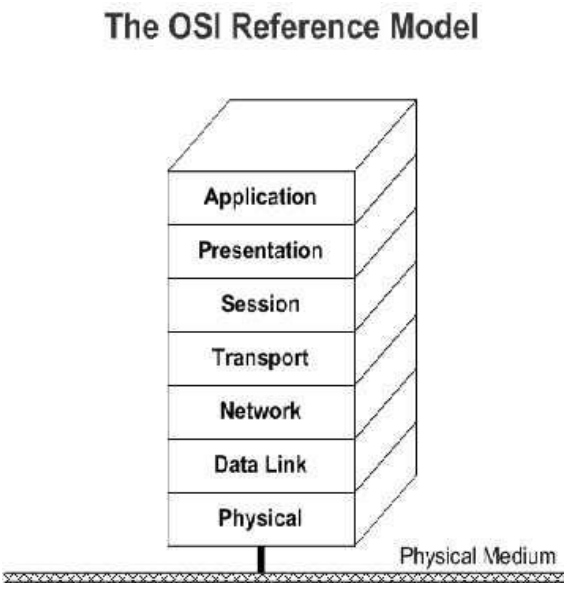
Gambar 2.4 Internet

2.1.4. Model *Osi Layer*

Model interkoneksi sistem terbuka, yang lebih dikenal sebagai model OSI, yang artinya peta jaringan yang ada awalnya dikembangkan sebagai standar *universal* untuk membuat suatu jaringan. Tetapi alih-alih melayani sebagai model

dengan protokol yang disetujui akan digunakan untuk seluruh dunia, model OSI telah menjadi alat pengajaran yang menunjukkan bagaimana tugas yang berbeda dalam suatu jaringan arus ditangani untuk mempromosikan data bebas kesalahan transmisi. Interkoneksi Sistem Terbuka model (Osi Model) yaitu model konseptual yang mencirikan dan menstadardisasi fungsi internal sebuah sistem komunikasi dengan mempartisipasi ke lapisan abstraksi (Chinmay, Vibhu; Garg 2015).

Model Osi bukanlah protokol, tetapi referensi model, atau struktur abstrak yang menggambarkan fungsi dan interaksi berbagai data protokol komunikasi. Ini memberikan konseptual struktur yang membantu kita mendiskusikan dan membandingkan jaringan fungsi, seperti bantuan sistem klasifikasi lainnya ahli biologi atau ahli kimia berbicara tentang bidang mereka. Sebagai *networking profesional*, ada dua alasan bagus anda harus memiliki pemahaman yang kuat tentang model OSI (Chinmay, Vibhu; Garg 2015).

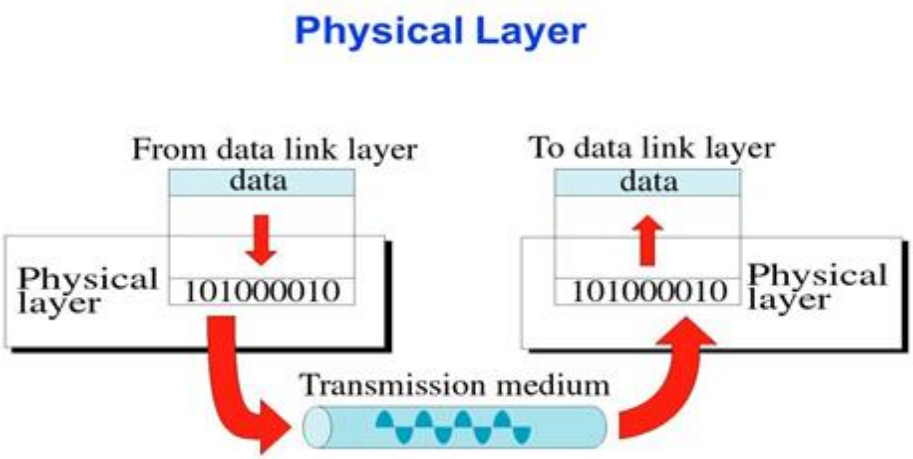


Gambar 2.5 Model *OSI Layer*

Tujuh lapis model *OSI* adalah :

1. Fisik (*Physical Layer*)

   Lapisan fisik adalah kabel, serat, atau kartu yang sebenarnya, *switch* dan mekanik dan listrik lainnya peralatan yang membentuk jaringan. Ini lapisannya yang dapat di ubah ke data digital menajdi sinyal yang dapat dikirim menyusuri kabel untuk mengirim data. Sinyal-sinyal ini sering listrik tetapi, seperti dalam kasus serat optic, mereka bias juga menjadi sinyal non-listrik seperti optic atau apapun jenis pulsa lain yang dapat dikodekan secara digital (Chinmay, Vibhu; Garg 2015).

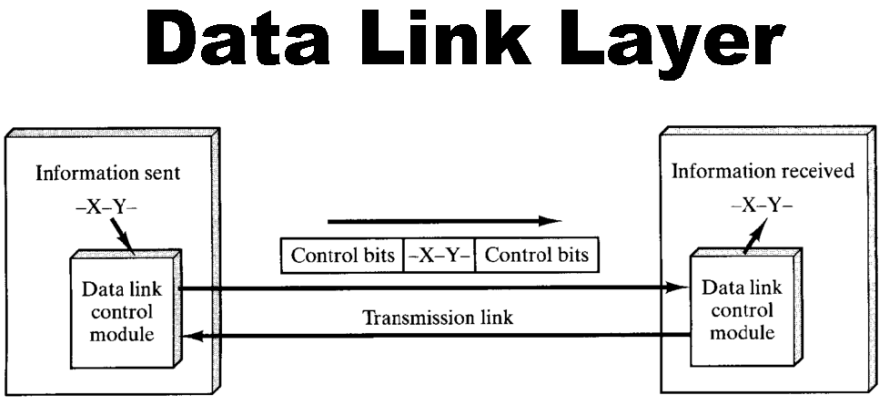


Gambar 2.6 Physical layer

2. Hubungan data (*Data Link Layer*)

   Lapisan tautan Data adalah tempat kumpulan informasi yang dikonversi ke dalam “paket” koheren dan binkai yang diteruskan kelapisan lebih tinggi. Pada dasarnya, lapisan data *link* membongkar data mentah yang berasal dari lapisan fisik dan menerjemahkan informasi dari beberapa

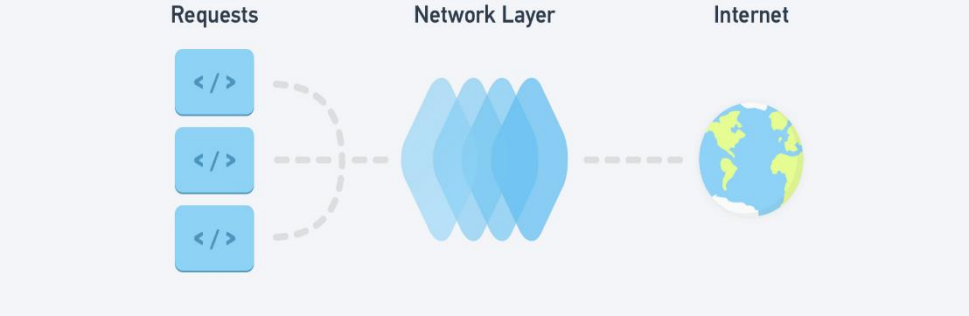
lapisan atas menjadi mentah data yang akan dikirim melalui lapisan fisik. Tautan daya *layer* juga bertanggung jawab untuk menangkap dan kompensasi untuk *ranyerrors* yang terjadi di fisik lapisan (Chinmay, Vibhu; Garg 2015).



Gambar 2.7 Data *Link Layer*

3. Jaringan (*Network Layer*)

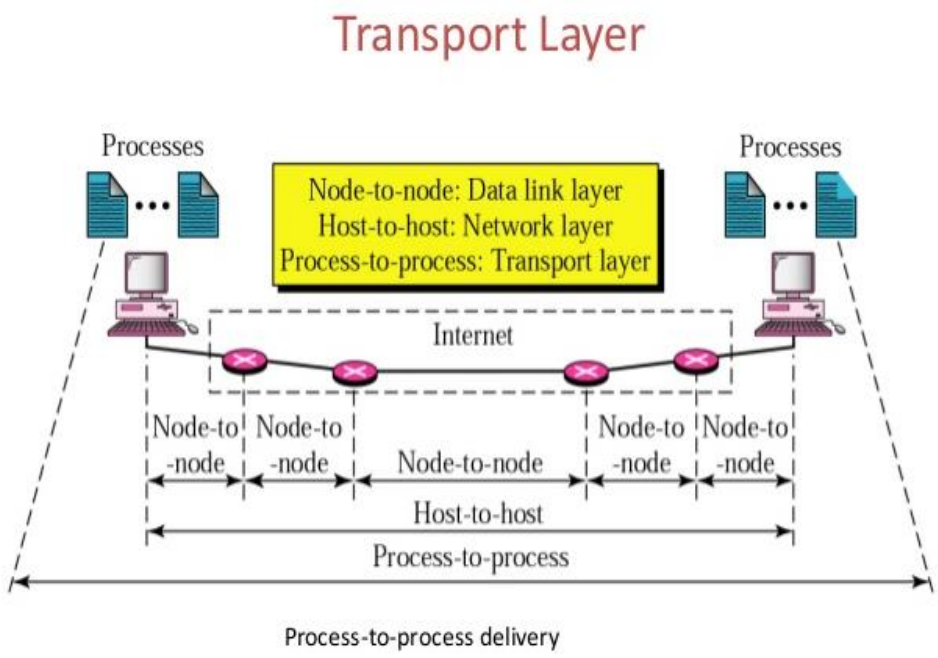
Lapisan jaringan adalah suatu tempat tujuan untuk data yang masuk dan keluar diatur. Ini adalah suatu lapisan di mana *router* bekerja untuk memastikan bahwa data itu benar-benar diatasi kembali sebelum meneruskannya ke kaki paket berikutnya perjalanan ini adalah lapisan di mana *router* bekerja untuk memastikan bahwa data benar-benar bisa diatasi kembali sebelum meneruskannya ke kaki paket berikutnya perjalan (Chinmay, Vibhu; Garg 2015).



Gambar 2.8 Network Layer

4. Transportasi (*Transport Layer*)

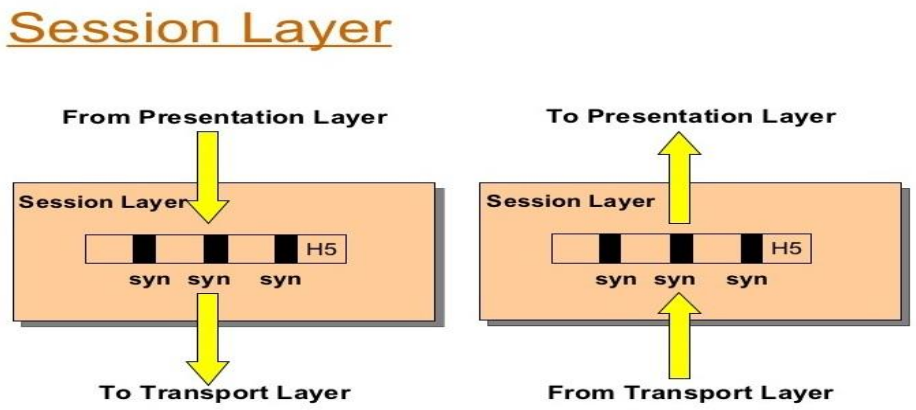
Lapisan transport bertanggung jawab untuk streaming data di seluruh jaringan. Pada level ini, datanya tidak memikirkan ke dalam hal paket individu tetapi lebih ke dalam hal percakapan. Untuk mecapai *level* ini, protokol-protokol yang didefinisikan sebagai aturan komunikasi adalah bekas. Protokol menyaksikan transmisi lengkap banyak paket memeriksa sebuah percakapan untuk kesalahan, mengakui transmisi yang sukses dan meminta pengiriman ulang jikan ada kesalahan terdeteksi (Chinmay, Vibhu; Garg 2015).



Gambar 2.9 Transport Layer

5. Sesi (*Session Layer*)

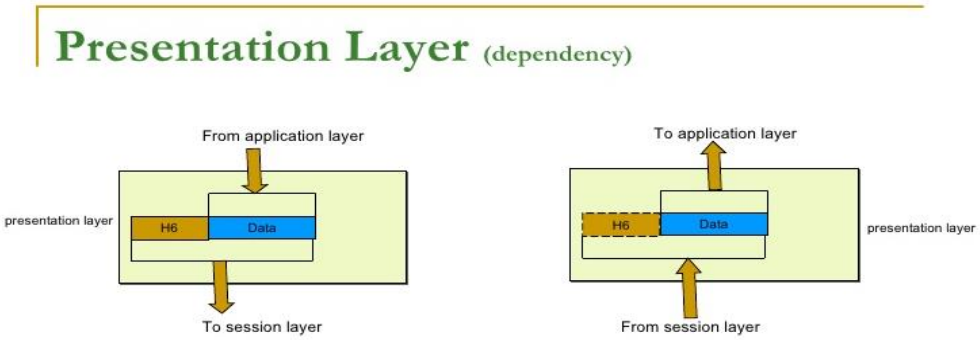
Lapisan sesi adalah tempat koneksi untuk dibuat, dipertahankan dan diakhiri. Ini biasanya mengacu pada permintaan aplikasi untuk data yang melalui jaringan. Sedangkan lapisan transport menangani aliran aktul data, lapisan sesi bertindak sebagai penyiar, membuat pastikan bahwa program dan aplikasi meminta dan mengirim data permintaan mereka yang di isi di istilah teknis, lapisan sesi menyinkronkan data transmisi (Chinmay, Vibhu; Garg 2015).



Gambar 2.10 Session Layer

6. Presentasi (*Presentation Layer*)

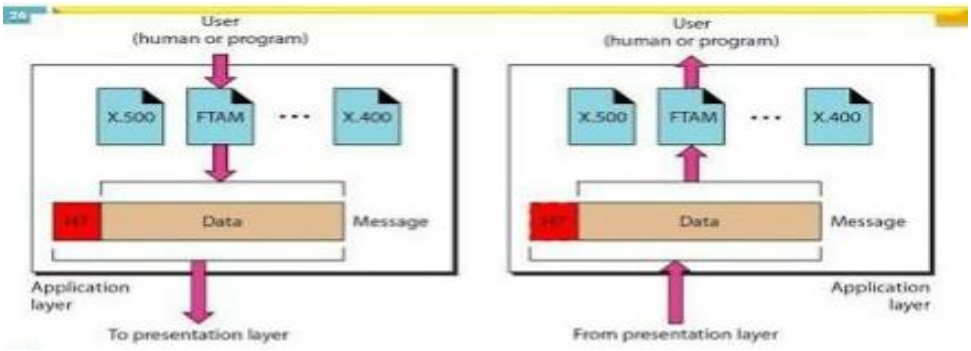
Lapisan presentasi adalah tempat data yang akan diterima dan akan diubah menjadi format aplikasi itu di takdirkan untuk biasa di mengerti. Pekerjaan yang dilakukan pada ini lapisan yang paling baik dipahami sebagai pekerjaan terjemahan. Untuk misalnya, data sering di enkripsi pada pressentasi lapisan sebelum di teruskan ke lapisan lain untu dikirim. Ketika data diterima, itu akan di dekripsi dan diteruskan ke aplikasi yang di tujukan untuk masuk ke format yang di harapkan (Chinmay, Vibhu; Garg 2015).



Gambar 2.11 Presentation Layer

7. Aplikasi (*aplication Layer*)

Lapisan aplikasi mengkoordinasikan akses jaringan untuk ke sebuah perangkat lunak yang akan dijalankan pada komputer tertentu atau alat. Protokol pada lapisan aplikasi ini menangani sebuah permintaan aplikasi perangkat lunak yang berbeda membuat ke jaringan. Jika menginginkan *browser Web* untuk mengunduh suatu gambar, klien email ingin memeriksa *server* dan *program-program file sharing* ingin mengunggah *file* film, protokol di lapisan aplikasi ini akan mengatur dan melaksanakan permintaan ini (Chinmay, Vibhu; Garg 2015).



Gambar 2.12 Aplication Layer

2.2. Teori Khusus

Peneliti akan membahas tentang suatu teori khusus terkait penelitian yang menggunakan beberapa kutipan yang di kutip oleh peneliti baik asal buku maupun jurnal penelitian sebelumnya :

Dalam teori khusus, menyebutkan variabel yang dipergunakan pada penelitian ini buat mendukung materi penelitian. Berikut merupakan konsep atau variabel yang menjadi latar belakang penelitian buat setiap indikator yang dapat dijelaskan.

1. *Wireshark*

Wireshark menurut (Diansyah 2015) di ibaratkan menjadi media atau tool yg bisa digunakan sang user, apakah untuk suatu kebaikan atau kejahatan. Hal ini sebab wireshark dapat pada gunakan buat mencari beberapa berita yang sensitif yg bisa berkeliaran dijaringan, contohnya istilah sandi, cookie serta lain sebagainnya.

Wireshark Network Protocol Analyzer adalah tool yang ditujukan buat penganalisisan paket data jaringan. *Wireshark* dilakukan untuk pengawasan terhadap suatu paket secara waktu nyata (*real time*) dan lalu mengambil data serta informasi dan menampilkan selengkap mungkin. *Wireshark* dipergunakan secara gratis karena perangkat lunak ini berbasis sumber terbuka. Aplikasi *wireshark* dapat berjalan di banyak *platform*, seperti *linux*, *windows* serta *mac* (Kadafi and Khusnawi 2015).

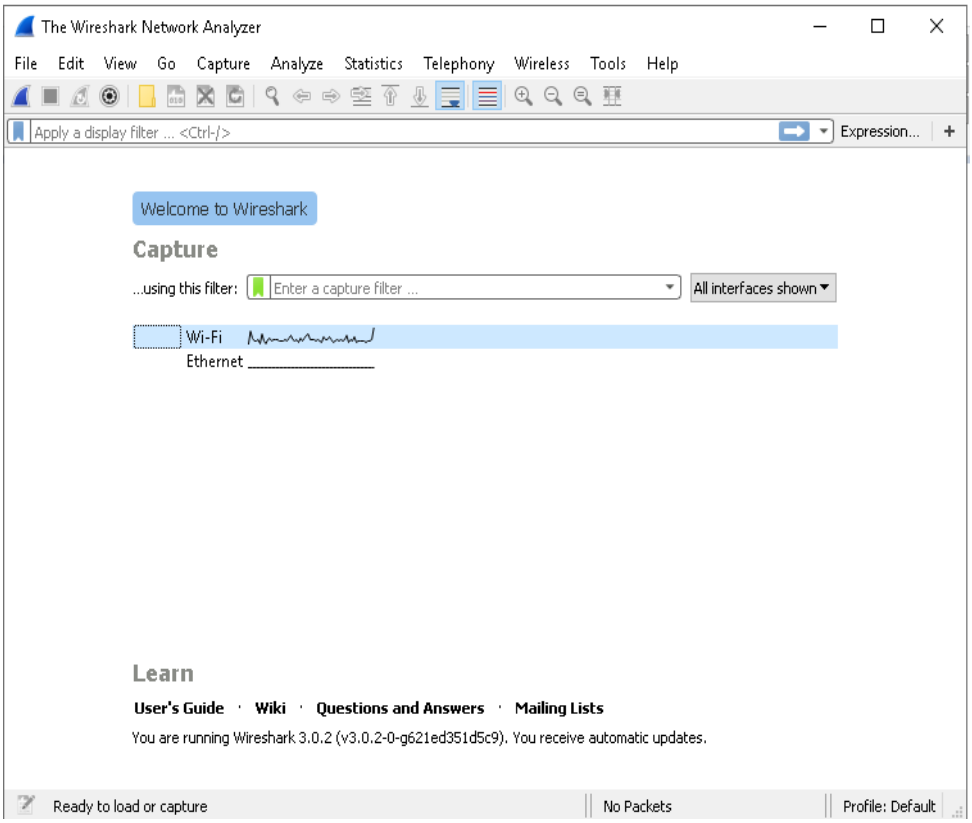
Wireshark Network Protocol Analyzer digunakan untuk mengamati *frame Ethernet*. Program ini di instal pada komputer yang menjalankan *Windows XP*. Program ini juga dapat digunakan sebagai sniffer, yang merupakan alat untuk menangkap sebuah komunikasi jaringan dalam waktu nyata untuk melihat hasil dalam *offline mode* dan menilai perilaku *frame Ethernet* yang tepat melewati pada *port switch, switch Ethernet* membutuhkan harus di konfigurasikan sehingga paket di kirim melalui port untuk menghubungkan sakelar ke perangkat "*sniffing*" (PC) (Kowalik, Rasolomampionona, and Januszewski 2017).

Proses *capture* paket dapat dilakukan ketika suatu topologi jaringan berhasil di bangun dengan terkoneksi dengan yang sangat baik. *Wireshark* mengizinkan pengguna mengamati suatu data dari jaringan yang tengah beroperasi serta dari data yang terdapat pada lokasi *disk*, serta segera melihat atau mensortir data yang tertangkap, mulai dari informasi singkat dan rincian buat segala hal perihal paket termasuk di dalamnya *full header* serta jumlah data yang dapat di peroleh (Azhar, Raisul; Hariyadi 2017).

2.3. Tools

Peralatan pendukung yang akan di pakai oleh peneliti dalam penelitian ini diantaranya :

1. Kebutuhan perangkat keras dan sistem operasi.
    a. Laptop HP EliteBook 840 G3. *Processor* i5 2,6 Ghz, RAM 8 GB, SSD 256 GB.
    b. *Wireless Network Card Broadcom* 802.11b/g/n *WLAN*.
    c. Sistem operasi *Windows* 10 *Pro.*
2. Kebutuhan Perangkat lunak.
    a. Sofware *Wireshark veri 3.0.2 64 bit*



Gambar 2.13 *Wireshark versi* 3.0.2

2.4. Penelitian Terdahulu

Berikut ini terdapat sejumlah model penelitian terdahulu dengan penelitian yang peneliti lakukan, meskipun ada sedikit perbedaan dengan penelitian peneliti ini :

1. Nama : Tengku Mohd Diansyah

   Judul : ANALISA PENCEGAHAN AKTIVITAS ILEGAL DIDALAM JARINGAN MENGGUNAKAN WIRESHARK

   ISSN/ISBN : 2337 – 3601

   Vol/No/Tahun : IV / 2 / 2015

Berdasarkan hasil penelitian yang dilakukan, disimpulkan bahwa dari data mendapatkan protocol jaringan dari hasil dari fitler paket data yang menggunakan aplikasi *wireshark* caranya relatif praktis membandingkan dengan software mirip forensic tools snort sebab membutuhkan pengaturan di snort.conf sedangkan di wireshark hanya relatif menentukan filter paket pada kolom filter. sehingga administrator jaringan dapat menganalisa paket jaringan yg sedang berlangsung.

2. Nama : Muamar Kadafi dan Khusnawi

   Judul : ANALISIS ROGUE DHCP PACKETS MENGGUNAKAN WIRESHARK NETWORK PROTOCOL ANALYZER

   ISSN/ISBN : 2354 – 5771

   Vol/No/Tahun : 2 / 2 / 2015

   Berdasarkan hasil penelitian yang dilakukan, dapat disimpulkan bahwa sistem kemananan jaringan yang dibangun dapat mendeteksi dan mencegah adanya Rogue DHCP Server di dalam jaringan DHCP berbasis Ipv4.

3. Nama : Muamar Kadafi dan Khusnawi

   Judul : SIMULATOR GNS3 DAN WIRESHARK SEBAGAI MODEL VIRTUAL PEMBELAJARAN PRATIKUM JARINGAN KOMPUTER

ISSN/ISBN : 2442 – 7667

Vol/No/Tahun : 16 / 3 / 2017

Sesuai akibat penelitian yg dilakukan, bisa disimpulkan bahwa desain model virtual pembejaran jaringan komputer dapat diterapkan dengan mengganti model konvensional (penggunaa perangkat phisik atau real) dengan hanya menggunakan satu buah komputer yang divirtualisasi dengan aplikasi virtual mesin (Vmware Workstation) dengan spesifikasi hardware yang sesuai dengan aplikasi yang dipergunakan Desain model virtual.

4. Nama : Vibhu Chinmay & Rishabh Garg

   Judul : A REVIEW PAPER ON OSI MODEL – A SEVEN LAYERED ARCHITECTURE OF OSI MODEL

   ISSN/ISBN : 2349 – 6002

   Vol/No/Tahun : 1 / 12 / 2015

   Berdasarkan hasil penelitian yang dilakukan, dapat disimpulkan bahwa pengembangan Standar OSI merupakan tantangan yang sangat besar, yang hasilnya akan mempengaruhi semua perkembangan komunikasi komputer di masa depan. Jika standar datang terlambat atau tidak memadai, interkoneksi sistem heterogen tidak akan mungkin atau akan sangat mahal.

5. Nama : Ryszard Kowalik, Désiré D. Rasolomampionona, & Marcin Januszewski

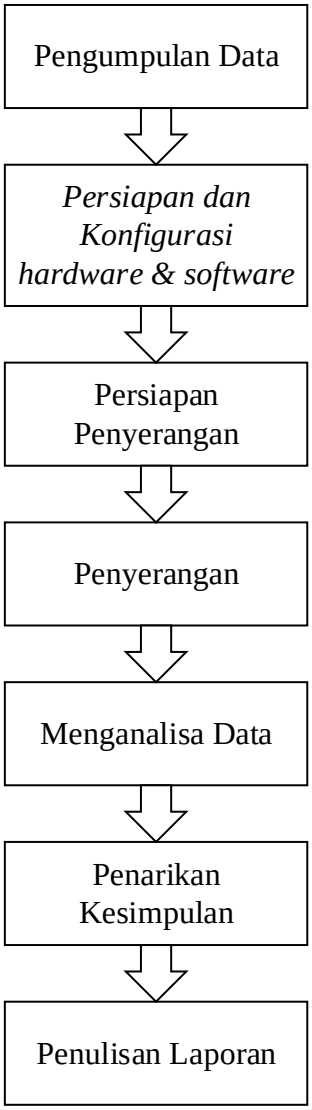
Judul : LABORATORY TESTING OF PROCESS BUS EQUIPMENT AND PROTECTION FUNCTIONS IN ACCORDANCE WITH IEC 61850 STANDARD : PART II : TESTS OF PROTECTION FUNCTIONS IN A LAN-BASED ENVIRONMENT

ISSN/ISBN : 0142 – 0615

Vol/No/Tahun : 94 / - / 2017

Berdasarkan hasil penelitian yang dilakukan, dapat disimpulkan bahwa dampak penundaan fungsi perlindungan sehubungan dengan penggunaan perangkat jaringan tambahan sangat minim. Perangkat jaringan tambahan telah memungkinkan untuk melipatgandakan koneksi telekomunikasi. Tidak ada perbedaan signifikan dalam pengukuran sinyal analog dan digital yang telah diamati ketika melakukan pengukuran dalam lingkungan LAN. Hal ini disebabkan oleh fakta bahwa proses sinkronisasi dan pengaturan waktu diatur oleh perangkat master (dalam hal ini relay D60), dan nomor informasi (frame) digunakan untuk mengidentifikasi instants waktu.

2.5. Kerangka Pemikiran



Gambar 2.14 Kerangka Pemikiran
Sumber: Peneliti

Sesuai menggunakan diagram alir penelitian diatas penelitian ini dilakukan pada beberapa tahapan.

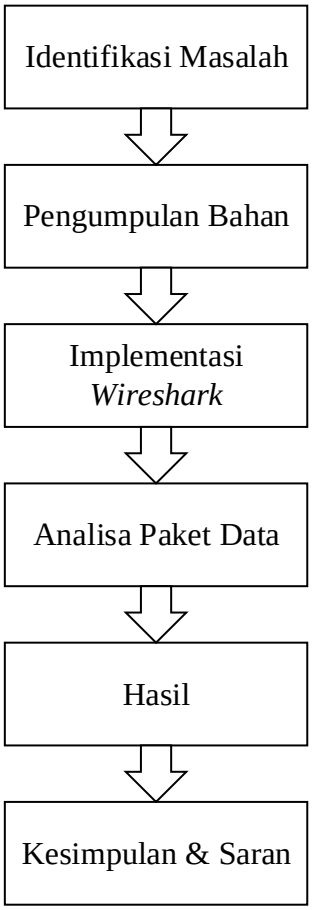
1. Pengumpulan data, merupakan proses *capture data* dari aplikasi *wireshark* terhadap jaringan komputer.
2. Persiapan dan Konfigurasi *hardware & software*, yaitu Laptop dan *Software wireshark* untuk persiapan melakukan penyerangan.
3. Persiapan penyerangan, yaitu memantau setiap pergerakan data yang mencurigakan.
4. Analisis serangan, menganalisa sebab timbulnya serangan pada jaringan komputer.
5. Penarikan kesimpulan, menjelaskan asal timbulnya serangan sampai dengan solusi untuk menyelesaikan masalah tersebut.
6. Penulisan laporan, yaitu membuat laporan hasil penelitian.

BAB III

METODE PENELITIAN

3.1. Desain Penelitian

Desain penelitian dapat dijabarkan seperti pada gambar berikut:



Gambar 3.1 Desain Penelitian
Sumber: Peneliti

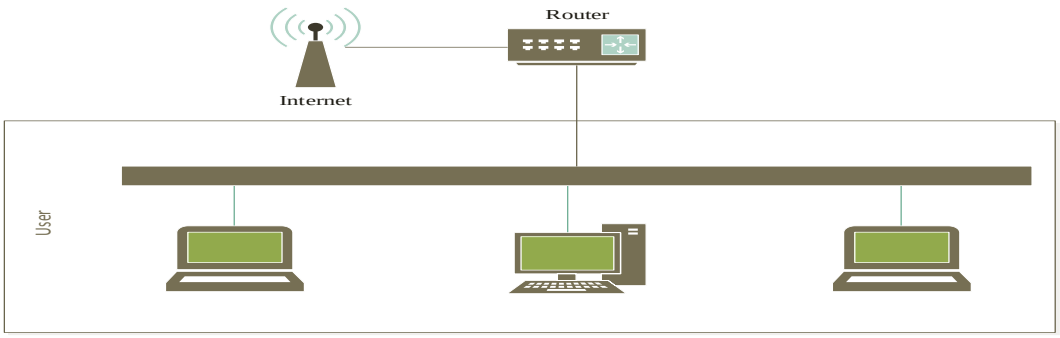
Berikut adalah pembahasan dari gambar pada atas :

1. Identifikasi masalah, artinya dasar pada penelitian yang telah dibahas pada bab 1.
2. Pengumpulan bahan, yang dibutuhkan dalam sebuah penelitian dari segi *hardware* dan *software*.
3. Implementasi *wireshark*, yaitu aplikasi untuk *capture* data dari jaringan komputer yang dianalisa.
4. Analisa paket data, menganalisa data yang telah di *capture* dari aplikasi *wireshark* untuk mengetahui serangan yang datang.
5. Penarikan kesimpulan.

3.2. Analisis Jaringan Lama/ yang Sedang Berjalan

Analisa jaringan yang sedang berjalan pada perusahaan yang diteliti merupakan tahapan yang penting agar bisa mengetahui alur jaringan yang digunakan. Berikut alur jaringan yang digunakan pada perusahaan yang akan diteliti :

1. Topologi Jaringan yang Sedang Berjalan



Gambar 3.2 Topologi Jaringan yang Sedang Berjalan

2. Hardware

Pada jaringan yang lama/sedang berjalan, ada beberapa perangkat keras yang sedang berjalan di Kantor Pemerintah Kota Batam. Berikut ini perangkat-perangkat keras yang sedang berjalan :

Nama Perangkat	Fungsi
Internet	suatu jaringan komunikasi yang menghubungkan satu media elektonik menggunakan media yang lainnya.
Router	menentukan jalur yang akan dilewati paket dari satu device ke device yang berada di dalam jaringan

Tabel 3.1 Perangkat Keras yang Sedang Berjalan

3. Policy/Kebijakan Bidang Jaringan yang Sedang Berjalan

Kebijakan pada jaringan digunakan sebagai manajemen keamanan di Kantor Pemerintah Kota Batam agar mendapatkan alur kerja yang baik, aman, dan tentram. Kebijakan di perusahaan yang diteliti mencakup hal-hal berikut ini :

1. Tidak adanya pengaturan pembagian kuota internet pada setiap komputer.
2. Pada internet/*wi-fi* di Kantor Pemerintah Kota Batam belum ada pembatasan pendaftaran menggunakan *MAC Address* sehingga pihak luar yang mengetahui password internet dapat langsung mengakses.

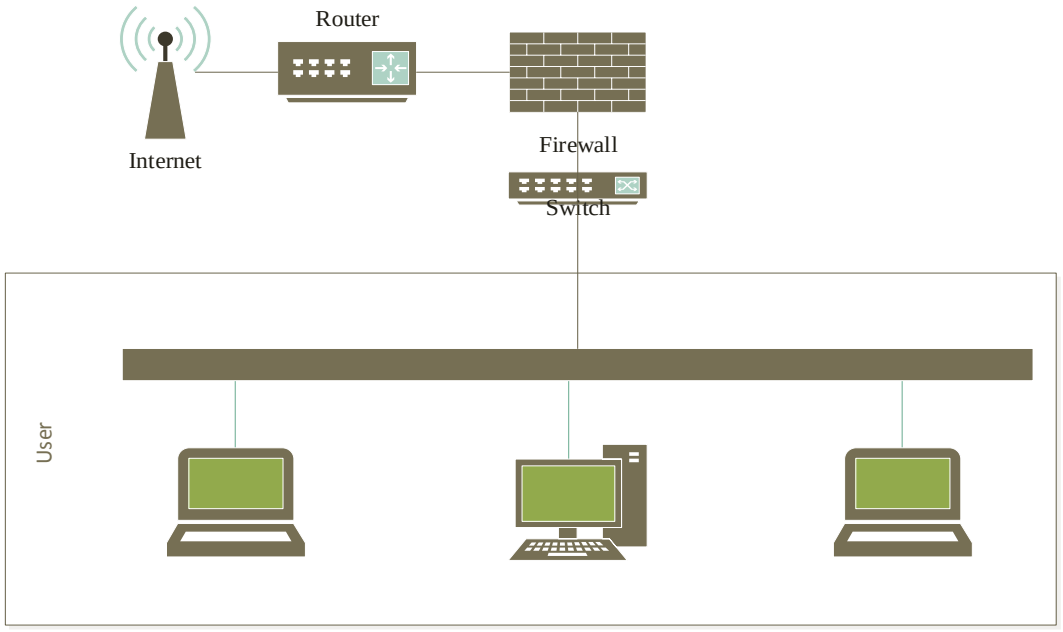
3. Tidak ada pemblokiran pada *file/software* pada setiap komputer sehingga *user* dapat *install/download* dengan bebas.

3.3. Rancangan Jaringan yang Dibangun/Diusulkan

Rancangan jaringan yang akan dibangun merupakan usulan dari peneliti agar mendapatkan hasil yang lebih efektif dan efisien dibanding jaringan yang sekarang dijalankan. Berikut usulan jaringan yang akan dibangun guna mendapat hasil yang lebih baik.

1. Topologi Jaringan yang Diusulkan

Topologi jaringan yang diusulkan oleh peneliti untuk digunakan pada perusahaan yaitu Topologi Star. Berikut gambaran dari topologi jaringan yang sedang digunakan.



Gambar 3.3 Topologi Jaringan yang Diusulkan

2. Hardware

Pada jaringan yang akan dibangun, terdapat beberapa perangkat keras yang diusulkan peneliti untuk digunakan di Kantor Pemerintah Kota Batam. Berikut ini perangkat-perangkat keras yang diusulkan :

Nama Perangkat	Fungsi
Internet	suatu jaringan komunikasi yang menghubungkan satu media elektonik dengan media yang lainnya.
Router	menentukan jalur yang akan dilewati paket dari satu device ke device yang berada di dalam jaringan
Firewall	Mengontrol dan mengawasi paket data yang mengalir di jaringan komputer.
Switch	Suatu jenis komponen jaringan komputer yang digunakan untuk menghubungkan beberapa *Switch/Router* dalam membentuk jaringan komputer yang lebih besar.

Tabel 3.2 Perangkat Keras yang Diusulkan

3.4. Lokasi dan Jadwal Penelitian

Pada penelitian ini, peneliti melakukan penelitian di Kantor Pemerintah Kota Batam, Penelitian ini dilaksanakan mulai dari bulan Maret 2019 sampai dengan bulan Juni 2019, rincian jadwal penelitian yang dilakukan dapat dilihat pada tabel jadwal penelitian berikut ini:

No	Kegiatan	Oktober				November				Desember				Januari			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Penentuan Judul dan Identifikasi Masalah																
2	Menentukan Kerangka Berpikir																
3	Menentukan Metode Penelitian																
4	Menganalisa Jaringan																
5	Membuat Kesimpulan																
6	Penyusunan Skripsi																

Tabel 3.1 Jadwal Penelitian