ANALISIS PROTOKOL PADA APLIKASI LINE DENGAN MENGGUNAKAN WIRESHARK NETWORK PROTOCOL ANALYZER

SKRIPSI

Oleh:

Landri Elusi Hutagalung

120210150

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KOMPUTER

UNIVERSITAS PUTERA BATAM

2018

ANALISIS PROTOKOL PADA APLIKASI LINE DENGAN MENGGUNAKAN WIRESHARK NETWORK PROTOCOL ANALYZER

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh:

Landri Elusi Hutagalung

120210150

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KOMPUTER

UNIVERSITAS PUTERA BATAM

2018

PERNYATAAN

Dengan ini saya menyatakan bahwa :

1. Skripsi ini adalah asli dan belum pernah diajukan untuk gelar akademik (sarjana, dan/atau magister), baik di Universitas Putera Batam maupun di perguruan tinggi lain.
2. Skripsi ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing.
3. Dalam skripsi ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi.

Batam, ...Februari 2018

Yang membuat pernyataan,

Landri Elusi Hutagalung

120210150

ANALISIS PROTOKOL PADA APLIKASI LINE DENGAN MENGGUNAKAN WIRESHARK NETWORK PROTOCOL ANALYZER

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh
Landri Elusi Hutagalung
120210150

Telah disetujui oleh Pembimbing pada tanggal
seperti tertera di bawah ini

Batam,…… Februari 2018

Cosmas Eko Suharyanto, S.Kom., M.MSI

Pembimbing

ABSTRAK

komunikasi dizaman modern seperti sekarang telah banyak mengalami perubahan berkirim pesan, voice call, video call. Salah satunya adalah Line Messanger yang merupakan salah satu instan messanger digunakan untuk berkirim pesan, gambar, suara, dan juga video secara real time. analisis yang dilakukan untuk mengetahui protokol apa saja yang mengalir di Line Messanger saat melakukan komunikasi satu sama lain. parameter dalam melakukan analisis protokol yang ada pada Line Messanger adalah memonitoring dengan menggunakan pc atau laptop menggunkan software pendukung yaitu Wireshark Network Protocol Analyzer yang bekerja melalui media interface pc atau laptop. analisis ini berguna untuk menangkap paket-paket jaringan dan berusaha untuk menampilkan semua informasi di paket tersebut secara detail.

kata kunci : Line Messanger, Protokol, Wireshrak

ABSTRACT

communication in modern times like now have been changed council has sent a message , voice call , video call .One of which is line messanger that is one instant messanger used to council has sent a message , pictures , sound , and also video in real time . The analysis was conducted to obtain protocol anything whereunder line messanger when communicating each other . Parameters in an analysis protocol is in line monitor messanger is using pc or laptop software that is both supporters wireshark network protocol analyzer working through the interface pc or laptop . This analysis useful to catch paket-paket networks and trying to display any information in the package in detail .

Keywords: line messanger , protocol , wireshrak

KATA PENGANTAR

puji syukur kita panjatkan kepada Tuhan Yang Maha Esa 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 Ibu Dr.Nur Elfi Husda, S.Kom., M.SI selaku Rektor Universitas Putera Batam
2 Bapak Andi Maslan, S.T.,M.SI selaku Ketua Program Studi pada Program Studi Teknik Informatika Universitas Putera Batam
3 Bapak Cosmas Eko Suharyanto, S.Kom.,M.MSI. selaku pembimbing Skripsi.
4 Dosen dan Staff Universitas Putera Batam
5 Orang tua,adik-adikku, serta keluarga besarku tercinta yang senantiasa mendoa’kan , memotivasi dan mengharapkan keberhasilan dan kebahagian, sekaligus dukungan moril maupun materil.

6 sahabat-sahabatku Desi, Anis, Yuni, dedi, diana, yanti dan teman-teman yang penulis tidak bisa sebutkan satu persatu atas dukungan terhadap penulis dalam pembuatan skripsi ini.

akhir kata penulis mengharapkan penyusunan skripsi ini semakin memperkaya ilmu pengetahuan bagi kalangan akademis dan menambah wawasan baru bagi kalangan praktisi serta bermanfaat bagi kita semua.

Batam, Februari 2018

Landri Elusi Hutagalung

DAFTAR ISI

HALAMAN SAMPUL DEPAN ..... **i**
HALAMAN JUDUL ..... **ii**
HALAMAN PERNYATAAN ..... **iii**
HALAMAN PENGESAHAN ..... **iv**
ABSTRAK ..... **v**
ABSTRACT ..... **vi**
KATA PENGANTAR ..... **vii**
DAFTAR ISI ..... **ix**
DAFTAR TABEL ..... **xii**
DAFTAR GAMBAR ..... **xiii**
DAFTAR LAMPIRAN. ..... **xiv**

BAB I PENDAHULUAN **1**

1.1.Latar Belakang Penelitian 1

1.2.Identifikasi Masalah 4

1.3.Pembatasan Masalah 5

1.4.Perumusan Masalah 5

1.5.Tujuan Penelitian 6

1.6.Manfaat Penelitian 6

1.6.1.Aspek teoritis (keilmuan) 6

1.6.2Aspek Praktis (Guna Laksana) 7

BAB II KAJIAN PUSTAKA **8**

2.1. Teori Dasar 8

2.1.1. Jaringan Komputer 8

2.1.2. Standar Jaringan Komputer 8

2.1.3. Jenis-Jenis Jaringan Komputer 11

2.1.4. Model OSI 16

2.2. Teori Khusus 17
2.2.1. Protokol Jaringan 17
2.2.2. Line 27
2.2.3. Network Forensic 30
2.3. Tool/software/aplikasi/*system* 30
2.3.1. Wireshark 31
2.3.2. Fitur *Wirshark* 32
2.3.3. Protokol-Protokol Yang Paket Datanya Dapat Di Identifikasi Oleh Wireshark. 32
2.4. Penelitian Terdahulu 34
2.5. Kerangka pemikiran 43
BAB III METODE PENELITIAN 45
3.1. Desain Penelitian 45
3.2. Operasional Variabel Penelitian 47
3.3. Objek Monitoring 47
3.4. Teknik Dan Alat Pengumpulan Data 48
3.4.1. Teknik Pengumpulan Data 48
3.4.2. Pengamatan Atau Observasi 48
3.4.3. Dokumentasi 50
3.5. Alat Pengumpulaan Data 50
3.6. Jadwal Penelitian 51
BAB IV HASIL PENELITIAN DAN PEMBAHASAN 52
4.1. Hasil Penelitian 52
4.2 Analisis Deskriptif Paket Data 54
4.2.1 Analisis Protocol Hierarchy 55

4.2.2 Analisis Conversation 57
4.2.3 Analisis Endpoint 57
4.2.4 Analisis Domain Name Service (DNS) 58
4.3 SSL 60
BAB V KESIMPULAN DAN SARAN 68
5.1. KESIMPULAN 68
5.2. SARAN 69
DAFTAR PUSTAKA
RIWAYAT HIDUP
SURAT KETERANGAN PENELITIAN
LAMPIRAN

DAFTAR GAMBAR

Gambar 2. 1 Topologi Bus 13
Gambar 2. 2 Topologi Ring 13
Gambar 2. 3 Topologi Star atau Bintang 14
Gambar 2. 4 Topologi Extended Star 14
Gambar 2. 5 Topologi Mesh 15
Gambar 2. 6Topologi Tree Atau Pohon 16
Gambar 2. 7 OSI Reference Model 20
Gambar 2. 8TCP Reference Model 27
Gambar 2. 9 Line Messenger 30
Gambar 2. 10Line Messenger 31
Gambar 2. 11 Kerangka Pemikiran 44
Gambar 3. 1 Desain Penelitian 46
Gambar 3. 2 Objek Monitoring 47
Gambar 4. 1 Diagram Paket Data Line Messenger 54
Gambar 4. 2 Analisis Domain Name System (DNS) 59
Gambar 4. 3 DNS Trafik Query 60
Gambar 4. 4 Icon kunci atau bar 61
Gambar 4. 5 Sertifikat SSL Line 62
Gambar 4. 6 Enkripsi Pada Line 63
Gambar 4. 7 Total Paket SSL Dalam 1 Bulan 64
Gambar 4. 8 TLSV1.2 65
Gambar 4. 9 Ethernet Frame 65
Gambar 4. 10 TCP 66
Gambar 4. 11 IPv4 67

DAFTAR TABEL

Tabel 2. 1 kelas IP 10
Tabel 2. 2IP Private 11
Tabel 2. 3 UPPER-LOWER Layer 21
Tabel 2. 4 Karakteristik OSI Layer 21
Tabel 3. 1 Alat Pengumpulan Data 50
Tabel 3. 2 Jadwal Penelitian 51
Tabel 4.1 *Tabel 4. 1* Paket data Line messanger 53
Tabel 4. 2 Total Paket Data 55
Tabel 4. 3 Protokol Hierachy 55
Tabel 4. 4 TCP Protokol Hierachy 56
Tabel 4. 5 Analisis Conversation 57
Tabel 4. 6 Analisis Endpoint 58

DAFTAR LAMPIRAN

Lampiran 1 : Tutorial menginstal software Wireshark

BAB I

PENDAHULUAN

1.1. Latar Belakang Penelitian

Di era yang berbasis internet sekarang ini, perkembangan teknologi pada dunia telekomunikasi juga semakin pesat, di antaranya dalam aplikasi berkirim pesan. karena orang-orang berada di tempat lain dan ingin berkomunikasi dengan orang yang berada di tempat lain yang jauh pula. Aplikasi berkirim pesan juga dapat digunakan sebagai media untuk berbagi status, pesan suara, foto, kontak, video sehingga terlihat sepertinya nyata. Salah satu contoh aplikasi berkirim pesan tersebut adalah aplikasi Line.

Line merupakan aplikasi *instant messaging* yang menggunakan sistem nomor telepon seluler penggunanya sebagai basis untuk saling berhubungan. Dengan memanfaatkan teknologi ini maka aktifitas akan menjadi lebih mudah, misalnya untuk mengetahui *tranding topic*, dan *event* penting lainnya. Pada saat sekarang ini banyak vendor yang memanfaatkan kesempatan ini sebagai sebuah layanan yang dapat digunakan untuk mendistribusikan digital *produknya* yang mengalir di atas protokol (IP) jaringan internet.

Protokol dalam jaringan merupakan sebuah standar yang mengatur terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih

titik komputer. Protokol di terapkan pada perangkat keras, perangkat lunak, atau kombinasi dari keduanya. Pada tingkat terendah, protocol mendefenisikan koneksi perangkat keras. Protokol di standarisasi oleh beberapa organisasi yaitu *IETF, ETSI, ITU,* dan *ANSI.*

OSI (Open System Interconnection) adalah suatu model konseptual yang terdiri atas tujuh layer, yang masing-masing layer tersebut mempunyai fungsi yang berbeda. OSI di kembangkan oleh badan Internasional yaitu ISO (International Organization for Standardization) pada tahun 1977. Model ini juga di kenal dengan model tujuh lapis OSI (*OSI seven layer model*). TCP/IP atau *Transmission Control Protocol/Internet Protocol* adalah sekumpulan protokol yang di desain untuk melakukan fungsi-fungsi komunikasi data pada *wide area network* (WAN). Pada TCP/IP memiliki empat layer. TCP/IP juga merupakan standar komunikasi data yang di gunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Berikut ini adalah beberapa protokol beserta fungsinya. HTTP *(Hyper Text Transfer Protocol), protokol yang di gunakan untuk web browsing di jaringan internet.* FTP (*File Transfer Protocol*), di gunakan untuk mentransfer file dalam jaringan internet. POP *(Post Office Protocol),* di gunakan untuk mengambil mail dari suatu server. RIP *(Routing Information Protocol),* di gunakan untuk keperluan routing. DNS *(Domain Name Service),* di gunakan untuk memmetakan alamat IP Address ke dalam nama atau group tertentu. MIME *(Multipurpose Internet Mail Extention),* di gunakan untuk mengirimkan *file bina*ry dalam bentuk teks pada suatu

jaringan. SMB *(Server Message Block),* di gunakan untuk mentransfer berbagai file dari sistem operasi DOS dan Windows. NFS *(Network File System),* di gunakan untuk *sharing file* bagi *host* berbagai jaringan dan sistem operasi. NNTP (*Network News Transfer Protocol),* di gunakan untuk mengirim dan menerima *Newsgroup*. DHCP (*Dynamic Host Configuration Protocol*), di gunakan untuk di stribusi nomor IP pada jaringan dengan jumlah ip terbatas, yang di sediakan oleh komputer server. TELNET (*Network Terminal Protocol),* di gunakan untuk melakukan remote login bagi pengguna jaringan. SMTP (*simple mail transfer protocol*), di gunakan untuk mengirimkan *E-Mail* di jaringan internet. SNMP (*simple network management protocol*), di gunakan untuk mengelola suatu jaringan. RPC (*remote procedure call*), di gunakan untuk memanggil dari jarak jauh. NETBIOS (*network basic input output system*), di gunakan untuk sebagai protokol standar dalam jaringan. ARP (*address resolution protocol*), di gunakan untuk mendapatkan informasi hardware dari nomor IP.

paket data lalu lintas masuk dan lalu lintas keluar dalam hal ini penulis meneliti pada aplikasi line. Penulis menggunakan aplikasi *wireshark network protocol analyzer* karena merupakan salah satu dari sekian banyak tool Network Analyzer yang banyak di gunakan oleh Network administrator untuk menganalisa kinerja jaringannya termasuk protokol didalamnya. *Wireshark* banyak di gunakan karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis. Wireshark mampu menangkap paket-paket data dalam jaringan. Semua jenis paket informasi dalam berbagai

format protokol pun akan dengan mudah di tangkap dan di analisa.Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang berguna bagi professional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan. Tool wireshark dapat menganalisa transmisi paket data dalam jaringan, proses koneksi dan transmisi data antar komputer.

Berdasarkan latar belakang di atas sehingga penulis ingin melakukan penelitian terhadap protokol pada aplikasi Line. Maka, penelitian ini di beri judul : "ANALISIS PROTOKOL PADA APLIKASI LINE MENGGUNAKAN WIRESHARK NETWORK PROTOCOL ANALYZER".

1.2. Identifikasi Masalah

Berdasarkan latar belakang di atas maka pada penelitian ini dapat di identifikasi masalah sebagai berikut:

1. mengidentifikasi protokol HTTPS/SSL yang mengalir pada saat pengiriman dan penerimaan pesan pada aplikasi *Line*.
2. Mengidentifikasi protokol pada DNS saat melakukan pengiriman dan penerimaan data berupa teks, suara, gambar dan saat melakukan video call pada aplikasi *Line*.

1.3. Pembatasan Masalah

Agar permasalahan lebih terarah dan tidak menyimpang , maka perlu

adanya pembatasan masalah. Adapun pembatasan masalah sebagai berikut :

1. Tidak membahas keseluruhan *item* yang di gunakan pada *software wireshark network protocol analyzer*.
2. Membahas cara kerja perangkat lunak/ *software wireshark network protocol analyzer* yang di gunakan untuk monitoring lalu lintas data.
3. Kinerja yang dibahas adalah hanya protokol-protokol yang dilalui oleh line pada saat melakukan aktivitas di *Line* antara satu dengan lainnya.
4. Tidak membahas koneksi *internet* yang melibatkan *provider* tertentu.
5. Aplikasi yang akan dianalisis adalah *Line.*

1.4. Perumusan Masalah

Berdasarkan latar belakang yang di ungkapkan di atas, maka perumusan masalahan yang dapat di paparkan oleh penulis adalah sebagai berikut:

1. Bagaimana proses mengidentifikasi protokol HTTPS/SSL yang mengalir pada saat pengiriman dan penerimaan pesan pada aplikasi *Line?*
2. Bagaimana mengidentifikasi protokol DNS saat melakukan pengiriman dan penerimaan data berupa teks, suara, gambar dan saat melakukan video call pada aplikasi *Line*?

1.5. Tujuan Penelitian

Tujuan penulisan tugas akhir ini adalah untuk memperoleh data dan

informasi tentang Analisis Protokol Pada Aplikasi Line Dengan Menggunakan Wireshark Network Protocol Analyzer. Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut :

1. Untuk proses mengidentifikasi protokol HTTPS/SSL yang mengalir pada saat pengiriman dan penerimaan pesan pada aplikasi *Line*
2. Untuk mengidentifikasi protokol DNS saat melakukan pengiriman dan penerimaan data berupa teks, suara, gambar dan saat melakukan video call pada aplikasi *Line*

1.6. Manfaat Penelitian

Adapun manfaat dari di lakukannya penelitian ini pada Analisis Protokol Pada Aplikasi Line Menggunakan Wireshark Network Protocol Analyzer adalah :

1.6.1. Aspek teoritis (keilmuan)

1. Sebagai bahan acuan dan pelajaran untuk penulis menganalisa serta mampu mendeskripsikan protokol-protokol apa saja yang mengalir pada saat mengakses *line*.
2. Dengan melakukan penelitian ini, penulis mendapat pengalaman dalam menyusun karya ilmiah dan menambah kemampuan untuk mengamati, mengkaji serta menilai antara teori dengan kenyataan yang terjadi di lapangan yang pada.

1.6.2 Aspek Praktis (Guna Laksana)

2. Untuk mengaplikasikan ilmu yang telah di peroleh selama perkuliahan, serta Penulis dapat lebih mengerti cara untuk memantau lalu lintas data pada sebuah jaringan.
3. Penelitian ini diharapkan dapat menjadi bahan acuan bagi peneliti selajutnya yang ingin melakukan penelitian mengenai protokol pada aplikasi.

BAB II

KAJIAN PUSTAKA

2.1.Teori Dasar

2.1.1. Jaringan Komputer

Menurut (Priyo Utomo, 2012) jaringan komputer merupakan sistem yang terdiri dari atas dua atau lebih komputer serta perangkat-perangkat lainnya yang saling terhubung. Media Penghubung tersebut dapat berupa kabel atau nirkabel sehingga memungkinkan para pengguna jaringan komputer melakukan pertukaran informasi, seperti berbagi *file,* dokumen, data serta menggunakan perangkat keras atau perangkat lunak yang terhubung ke jaringan komputer.

2.1.2. Standar Jaringan Komputer

Menurut Setianto (2008:3) Jaringan komputer mirip dengan sebuah perkumpulan atau kelompok yang terdiri atas banyak anggota dengan latar belakang yang berbeda-beda. Agar dapat berkomunikasi dengan baik, kelompok tersebut membutuhkan sebuah aturan standar yang di sepakati

bersama, misalnya dalam penggunaan bahasa standar yang sama. Jika bahasa yang berbeda tetap di gunakan maka kelompok tersebut memerlukan *interpreter* atau penerjemah agar semua kelompok dapat memahaminya. Dalam dunia komputer dan komunikasi, bahasa atau penerjemah disebut dengan istilah protokol. Untuk membuat sebuah protokol yang baku di perlukan sebuah referensi atau pedoman yang di sebut OSI (*Open System Interconnection*). Pedoman OSI di harapkan dapat di gunakan sebagai referensi bagi semua vendor perangkat komputer dan telekomunikasi dalam mengembangkan protokolnya.

Menurut (Ilmiah et al., 2014) Pengalamatan IP (*IP Address*) Untuk bisa berkomunikasi pada suatu jaringan *private* ataupun pada jaringan *public Internet*, setiap *host* pada jaringan harus di identifikasi oleh suatu *IP address*. perlunya *IP address* bisa di pahami dalam kenyataannya bahwa :

1. Setiap perangkat atau *host* pada suatu jaringan memerlukan suatu *IP address* yang unik dalam segmen jaringan Setiap segmen fisik jaringan memerlukan suatu *address* unik pada jaringan tersebut.
2. *IP address* terdiri dari *ID* jaringan dan *ID host.*
3. *Subnetmask* menentukan seberapa banyak IP address yang bisa di buat dalam segmen jaringan.
4. IPv4 *(IP address version 4)* terdiri dari 32-bit number, biasanya ditulis dalam notasi decimal seperti :192.168.200.100.

IP Address bisa di kelompokkan dalam *Class IP* seperti dalam table 2.1, sementara dalam penerapan implementasi biasanya hanya di pakai *class* A, B, dan C saja.

Tabel 2. 1 kelas IP

Type	**Start Address**
Class A	1.0.0.0
Class B	128.0.0.0
Class C	192.0.0.0
Class D	224.0.0.0
Class E	240.0.0.0

IP address secara fungsi di kelompokkan dalam dua golongan IP address :

1) *Public IP address*, adalah *IP address* yang secara global merupakan *IP address* yang terhubung dalam jaringan Internet. Untuk mendapatkan *IP public* ini harus mendaftar ke *registrar* pemberi *IP Public*. Untuk wilayah *Asia Pasific IP Public* di keluarkan oleh APNIC (*Asia Pasific*

Network Information System). Kelompok-kelompok *IP public* yang bisa di gunakan di jaringan internet wilayah *Asia Pasific* di beli & dialokasikan dari APNIC.

2) *Private IP Address*, di batasi oleh range tertentu yang bisa di pakai oleh jaringan private akan tetapi tidak dapat di lihat oleh *public Internet. Internet Assigned Numbers Authority* (IANA) telah mengalokasi *IP address private* yang tidak pernah di pakai dalam global Internet. Tabel 2.2 berikut ini adalah *table Private IP address* yang bisa di gunakan dalam jaringan *private* yang hanya bisa di pakai untuk komunikasi ke dalam suatu *intranet*.

Tabel 2. 2*IP Private*

Class type	Start Address	End Address
Class A	10.0.0.0	10.255.255.254
Class B	172.16.0.0	172.31.255.254
Class C	192.168.0.0	192.168.255.254

2.1.3. Jenis-Jenis Jaringan Komputer

Menurut (Priyo Utomo, 2012) jenis jaringan komputer di bagi dalam beberapa kategori :

1 Berdasarkan Ruang Lingkupnya

1) *Local area network* (LAN), merupakan jaringan komputer yang di bangun di ruang lingkup kecil seperti sebuah perkantoran, rumah, atau institusi tertentu. LAN di bangun di ruang lingkup yang terbatas, hanya pada radius beberapa meter atau kilometer saja. Pembuatan sebuah LAN cukup sederhana.
2) *Metropolitan area network (*MAN), seperti namanya, jaringan komputer ini di bangun untuk kebutuhan ruang lingkup yang besar, bisa mencakup satu kota.
3) *Wide area network* (WAN), merupakan jaringan komputer dengan mencakup area yang lebih luas dan biasanya akan menghubungkan beberapa kesatuan jaringan komputer yang lebih banyak. Sebagaimana telah di jelaskan sebelumnya, koneksi antar jaringan dengan cakupan yang luas tersebut akan memudahkan kita berbagi sumber daya yang ada sehingga proses berbagi antar komputer atau jaringan dapat di lakukan secara lintas daerah, kota, negara, bahkan benua.

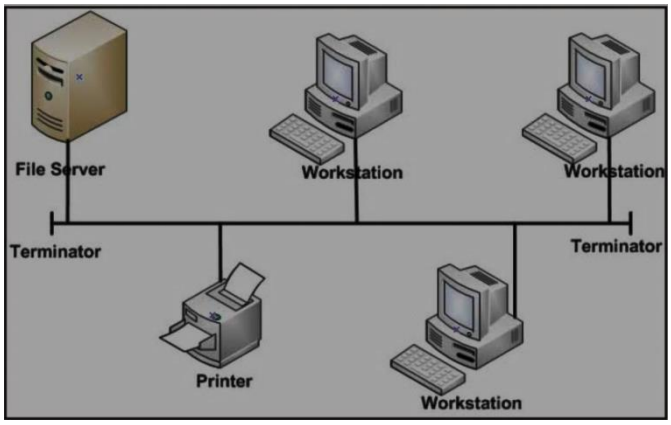
2 Berdasarkan Topologi

Topologi yang di maksud adalah gambaran struktur jaringan komputer yang akan di buat, berdasarkan topologinya, di bedakan menjadi enam, yaitu:

1) Topologi Bus

Jenis topologi ini menghubungkan setiap komputer/node dengan sebuah kabel komunikasi melalui sebuah kartu antarmuka (*card interface)* interface. setiap komputer dapat berhubungan dengan komputer lain yang ada dalam

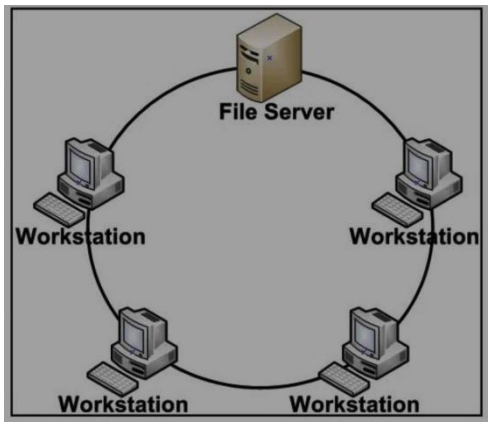
jaringan tersebut. Artinya, semua komputer mempunyai kedudukan yang sama dalam jaringan dan tidak tergantung pada komputer *server* pusat.



Gambar 2. 1 Topologi Bus

2) Topologi Ring

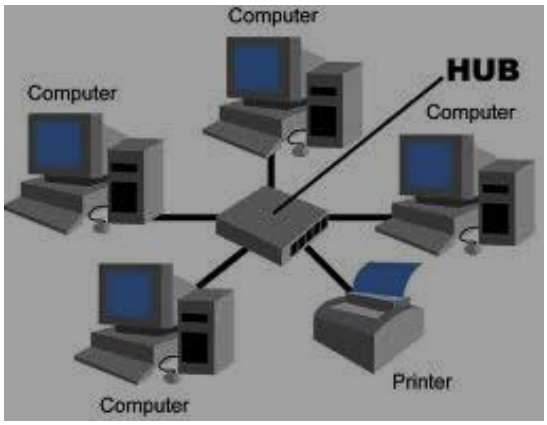
Komputer-komputer dalam jenis topologi ini akan di hubungkan dengan sebuah kabel dan membentuk seperti sebuah cincin. Pada jaringan ini tidak terdapat komputer pusat sehingga semua komputer mempunyai kedudukan yang sama. Data yang akan di kirim akan melewati beberapa simpul yang ada sampai pada simpul yang di tuju.



Gambar 2. 2 Topologi Ring

3) Topologi Star Atau Bintang

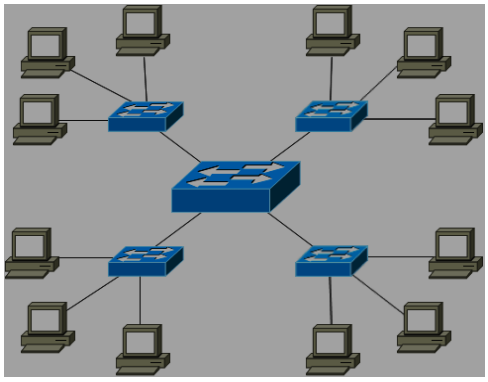
Dalam jenis topologi ini, beberapa komputer akan di hubungkan dengan satu pusat komputer sehingga semua kontrol berbagi sumber daya (*resource*) dalam jaringan yang di perlukan juga akan di pusatkan pada satu titik.



Gambar 2. 3 Topologi Star atau Bintang

4) Topologi Extended Star

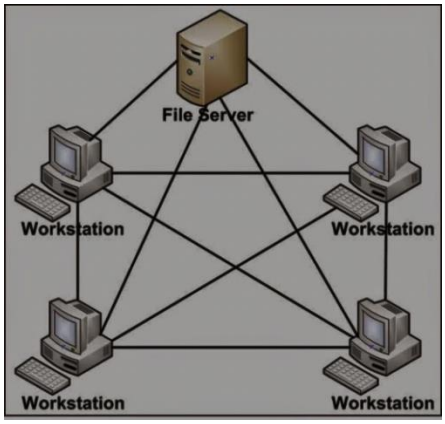
Dasar jenis topologi ini adalah topologi bintang, hanya di tambah pengulang (*repeater*) berupa hub atau pengalih (*switch*) sehingga memperluas jaringan yang jaraknya berjauhan.



Gambar 2. 4 Topologi Extended Star

5) Topologi Mesh

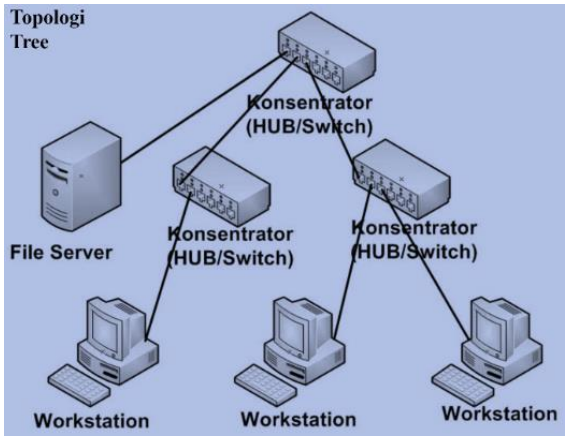
Jaringan dengan jenis topologi ini mempunyai jalur ganda pada setiap node/simpul. semakin banyak jumlah komputer yang ada dalam jaringan, semakin sulit pemasangan kabel-kabelnya, pemasangan kabel akan berlipat ganda.



Gambar 2. 5 Topologi Mesh

6) Topologi Tree Atau Pohon

Topologi jenis ini merupakan kombinasi antara topologi bintang dan topologi bus. topologi ini terdiri atas kumpulan topologi bintang yang di hubungkan dalam satu topologi bus sebagai jalur *backbone.*



Gambar 2. 6 Topologi Tree Atau Pohon

3. Berdasarkan Fungsi

1) Jaringan *Client-Server*

Pada jaringan ini terdapat satu komputer yang di siapkan sebagai komputer server yang akan melayani komputer lainnya yang berfungsi sebagai *client.*

2) Jaringan *Peer To Peer*

Pada jaringan ini sebuah komputer langsung di hubungkan ke komputer lainnya dan dapat saling berbagi pakai sumber daya (perangkat keras dan perangkat lunak) pada masing-masing komputer.

2.1.4. Model OSI

Menurut (Kurniawan, 2012) model *open system interconection* (OSI) telah di kembangkan oleh *international organization for standarization* (ISO) sebagai model dari arsitektur komunikasi komputer dan sebagai kerangka kerja untuk pengembangan standar protokol. terdiri dari tujuh layer yaitu :

1) *Application*

   Berfungsi untuk menyediakan akses ke lingkungan OSI oleh pengguna dan juga menyediakan informasi distribusi.

2) *Presentation*

   Berfungsi untuk menyediakan independensi untuk proses aplikasi dari perbedaan sintaksis format data.

3) *Session*

   Berfungsi untuk menyediakan struktur kontrol komunikasi antara aplikasi dan mengakhiri koneksi (sesi) antaraplikasi bersama.

4) *Transport*

   Berfungsi untuk keandalan dari transfer data antar titik akhir (*end point*), mengoreksi kesalahan data, dan mengatur aliran data.

5) *Network*

   Berfungsi sebagai layer atas dengan independeensi dari transmisi data dan teknologi pengalihan (*switching*) yang di gunakan oleh sistem untuk berkoneksi, yang mempunyai tugas untuk membangun, memelihara, dan mengakhiri koneksi.

6) *Data link*

   Berfungsi untuk transfer data informasi pada hubungan fisik seperti mengirim data, mengeblok data, dan lain-lain.

7) *Physical*

   Berhubungan dengan fisik seperti peralatan komunikasi, misalnya komputer, hub, router, kabel, dan lain-lain.

2.2.Teori Khusus

2.2.1. Protokol Jaringan

Menurut (Rafiudin, 2006) protokol merupakan istilah standard dalam konteks komunikasi data di antara mesin-mesin dalam jaringan. Protokol memungkinkan data di ambil dan di hantarkan bagian perbagian agar di peroleh transmisi yang lebih cepat dan *realibel*, kemudian di padukan kembali dalam susunan yang tepat begitu sampai di tujuan. Proses pemaduan di kenal dengan *reassembly*. Ketika data hendak di transmisikan di antara dua atau lebih *device* protokol bertanggung jawab dalam menjaga keutuhannya antara lain untuk memberikan cara mengecek error, mengenali jenis tekanan, memberikan cara bagi pengirim untuk mengenali akhir transmisi, dan memberikan cara bagi penerima untuk mengenali bahwa pesan telah di terima.

Protokol internet pertama kali di rancang pada awal tahun 1980-an. Akan tetapi pada saat itu protokol tersebut hanya di gunakan untuk menghubungkan beberapa *node* saja dan tidak di prediksikan akan tumbuh secara global seperti saat ini. Baru pada awal tahun 1990-an mulai di sadari bahwa internet mulai tumbuh keseluruh dunia dengan pesat. Sehingga mulai banyak bermunculan berbagai jenis protokol yang di gunakan untuk beberapa kalangan tertentu. Dengan terciptanya banyak jenis protokol, maka

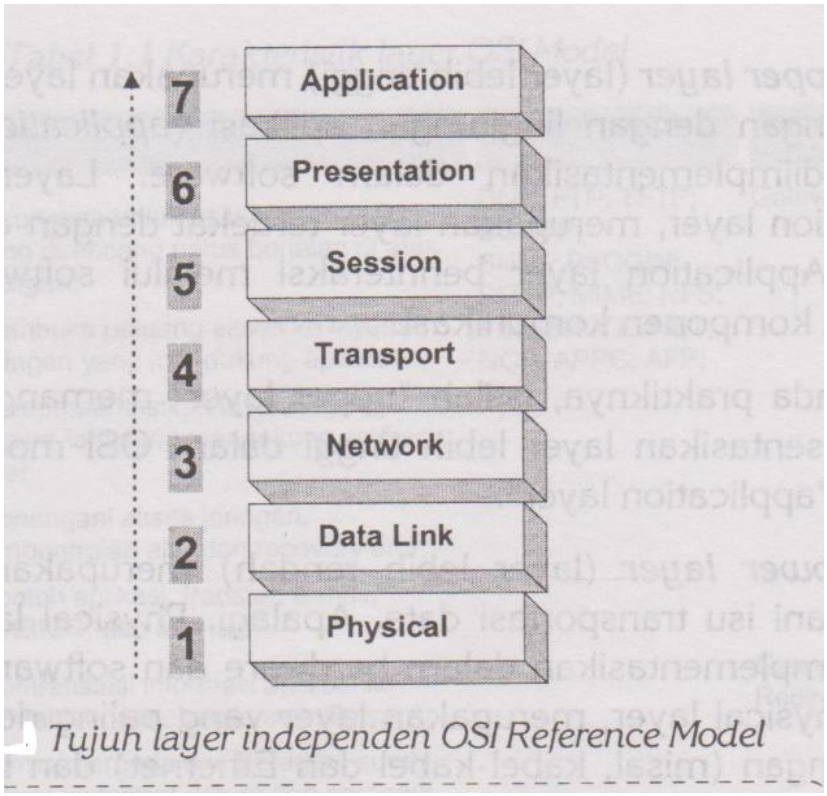
timbul suatu masalah baru dimana jenis protokol dari sebuah pabrik tertentu tidak dapat saling berkomunikasi terhadap protokol jenis lain. Sehingga pada akhirnya suatu badan, yaitu *international standard organization* (ISO) membuat standarisasi protokol yang saat ini di kenal dengan protokol model *Open System Interconnection* atau yang dikenal dengan OSI. Tetapi di karenakan model OSI ini adalah sebagai konsep dasar dan referensi teori cara bekerja sebuah protokol, dalam perkembangannya protokol TCP/IP di gunakan sebagai standar *De Facto*, yaitu standar yang di terima karena pemakaiannya secara sendiri semakin berkembang.

1. *Open System Interconnection* (OSI) Reference Model

Pembahasan protokol internet tidak akan lepas dari spesifikasi yang di tawarkan OSI. *Open system interconettion* (OSI) pada prinsipnya menjelaskan bagaimana informasi yang di lepaskan sebuah *software* aplikasi dalam komputer bergerak (melintasi media jaringan) ke sebuah software aplikasi dalam komputer lainnya (Rafiudin, 2006).

OSI *reference* merupakan sebuah model konseptual yang terdiri atas tujuh layer komunikasi, dimana masing-masing layer menetapkan fungsi khusus dalam jaringan. Model dikembangkan dan diperkenalkan secara luas oleh internationl organization for standarization (ISO) sekitar tahun 1984 dan sekarang telah menjadi model arsitektural utama dunia dalam komunikasi interkomputer.

Menurut (Rafiudin, 2006) OSI model membagi-bagi tugas penanganan informasi di antara komputer-komputer dalam jaringan kedalam 7 kelompok tugas yang lebih kecil, lebih praktis, dan mudah dikelola, yaitu :



Gambar 2. 7 OSI Reference Model

Menurut Kurniawan (2012:8) model OSI dengan tujuh layer sebenarnya dibagi menjadi dua kategori, yaitu layer atas (*upper layer*) dan layer bawah (*lower layer*). Layer atas umumnya berhubungan dengan aplikas yang di implementasikan dalam perangkat lunak. Biasanya layer teratas (*layer application*) juga menggunakan aplikasi perangkat lunak untuk berhubungan dengan pengguna akhir (*end user*). Sementara layer bawah berfungsi untuk menangani data *transport.*

Tabel 2. 3 UPPER-LOWER Layer

UPPER LAYERS	**APLICATION LAYER** Message Format, Human-Machine interface	E-mail Programs,Web Browsers,Photo Application, search enginers,Protocols : FTTP, FTP, SMTP
	PRESENTATION LAYER Coding into 1s and 0s;encryption,Compression	JPEG, MIDI,MPEG,PICT,TIFF, GIF
	SESION LAYER Authentication, Premission, Session Registration	concurrent database access, SQL,RPC, NFS
LOWER LAYERS	**TRANSPORT LAYER** End-to-end error control	TCP/UDP
	NETWORK LAYER Network Adressing : Routing or Switching	Routers and layer switches, Protocols : IPSec, ARP, ICMP
	DATA LINK LAYER Error detection, flow control on physical link	Bridge and Layer 2 switches, NIC/network adater, Protocol : MAC
	PHYSICAL LAYER Bit Stream Physical Medium, Method of Representing bits	Network port, cablesand power, layer 1 specs : DSL, Fibre Optic

Menurut Rafiudin (2008:4) masing-maasing layer dari tujuh layer OSI model memiliki karakteristik tersendiri sebagai berikut :

Tabel 2. 4 Karakteristik OSI Layer

LAYER	FUNGSI	PROTOKOL-PROTOKOL	KOMPONEN NETWORK
APLICATION	1.digunakan untuk aplikasi, terutama	DNS ; FTP;TFTP;BOOTP	Gateway
User Interface	yang dirancang untuk berjalan diatas	SNMP;RLOGIN;SMTP;	
	jaringan.	MIME;NFS;FINGER;	
	2.Membuka peluang akses kelayanan	TELNET;NCP;APPC;AFP;	
	jaringan yang mendukung aplikasi.	SMB	
	3.mempresentasikan layanan yang		
	secara langsung mendukung aplikasi		
	user.		
	4.menangani akses jaringan,		
	pengontrolaan alur dan recovery error		
	5.contoh aplikasi: transfer, e-mail,		
	NetBIOS,dan lain-lain.		
Presentation	1. mentranslasikan informasi aplikasi		Gateway
Translation	keformat jaringan,begitu sebaliknya.		Redirector
	2.format berbeda dari beragam sumber		
	dibua ke format umum dan seragam		
	yang dapat dipahami oleh OSI model.		
	3.bertanggung jawab atas konversi		
	protokol,konversi karakter, enskripsi		
	atau dengan dekripsi data, perluasan		
	perintah grafis, kompresi data.		
	4.mengeset standar untuk sistem		
	berbeda guna memberikan komunikasi		
	tanpa-kelim untuk stack protokol.		
	5.tidak selalu diimplementasikan dalam		
	protokol jaringan.		
Session	1.memulai, merawat,dan mengakhiri sesi	NetBIOS	Gateway
"syncs and sessions"	komunikasi jaringan	NAMES PIPES	
	2.bertanggung jawaab dalam	Mail Slots	

	pengenalan		
	nama (identifikasi), sehingga hanya	RPC	
	partai tertentu yang dapat berpartisipasi		
	dalam sesi.		
	3.memberikan layanan sinkronisasi		
	dengan merancang poin pengecekan		
	(checkpoint) dalam arus data. Jika sisa		
	rusak, maka hanya data setelah check		
	point terakhir yang perlu ditransmisikan.		
	4.mengatur siapa yang dapat mentrasmisi		
	data pada suatu waktu tertentu dan		
	untuk beberapa lama.		
Transport	1. koneksi tambahan yang berperan	TCP, ARP, RARP;	Gateway
packets; flow control	dibawah Session-layer	SPX	Advanced Cable
and error handling	2.mengelola flow control data diantara	NWLink	Tester
	partai-partai jaringan	NetBIOS/NetBEUI	Brouter
	3.membagi arus data ke dalam potongan	ATP	
	lebih kecil (yang dikenal pake) dan		
	Transport layer pada komputer penerima		
	melakukan reassembly paket menjadi		
	pesan seperti semula.		
	4.memberikan kapabilitas pengecekan		
	error guna menjamin penghantaran data		
	yang bebas error, baik hilang maupun		
	tergandakan.		
	5.memberikan kapabilitas		
	"acknowledgement" atas transmisi yang		
	sukses; meminta ulang jika beberapa		
	paket mendarat dengan cacat.		
	6.memberikan penanganan error dan		
	flow control		
Network	1.mentraanslasikan address network	IP, ARP, RARP	Brouter
Adressing, Routing	logikal beserta nama kebentuk address	ICMP, RIP,OSFP	Router
	fisikal. (namapc=> MAC Address)	IGMP	Frame relay
	2.bertanggung jawab untuk :	IPX	Device

	addressing,		
	penetapan rute pengiriman, penanganan	NWLink	ATM switch
	permasalahan jaringan.	NetBEUI	Advanced Cable
	3.jika router tidak dapat mengirim frame	OSI	Tester
	data dalam ukuran yang dikirim komputer	DDP	
	sumber, network layer menanganinya	DECnet	
	dengan memecah data kedalam unit yang		
	lebih kecil.		
Data Link	1.memutar paket ke dalam bit 100101	logical link contol : koreksi	Bridge
data frame to bits	dan pada mesin penerima mengembalikan	error dan flow control, mengelola	switch
	bit-bit ke dalam paket.	link control dan menetapkan SAP	ISDN Router
	2.menangani frame data diantara network	802.1 OSI Model	intelligent HUB
	layer dan physical layer.	802.2 logical link control	NIC
	3.meenerima paket data dari physical	media accescontrol: berkomunikasi	Advanced Cable
	layer (ke dalam frame data), kemudian	dengan card adapter, mengontrol	Tester
	dihantarkan ke network layer	tipe media yang digunakan	
	4.bertanggung jawab atas keutuhan	802.3 CSMA/CD/ethernet	
	frame yang ditransfer ke komputer lain	802.4 token Bus/ARCnet	
	dengan melintasi physical layer.	802.5 token ring	
		802.12 demand priority	
Physical	1.mentrasmisi arus bit melintasi media	IEEE 802	Reapeter
hardware ,raw bit stream	kabel	IEEE 802.2	multiplexer hub : passsive,
	2.menetapkan tipe kabel, card, dan aspek	ISO 2210	active
	fisikal lainnya.	ISDN	TDR
	3.menangani pemasangan NIC ke hardware		Oscilloscope
	dan bagaimana kabel dipasang ke NIC.		amplifier
	4.menetapkan teknik mentransfer arus bit		
	ke kabel.		

2. TCP/IP

TCP/IP (*transmission control protocol l/internet protocol*) adalah sekelompok protokol yang mengatur komunikasi data komputer di internet (Maslan, 2012). Komputer-komputer yang terhubung ke internet berkomunikasi

dengan protokol ini. Karena menggunakan bahasa yang sama, yaitu protokol *TCP/IP*, perbedaan jenis komputer dan sistem operasi yang tidak menjadi masalah komputer dengan *system operasi windows* dapat berkomunikasi dengan komputer mancintosh atau dengan *Sun Sparc* yang menjalankan solaris. Jadi jika sebuah komputer menggunakan protokol TCP/IP dan berhubungan langsung ke internet, maka komputer tersebut dapat terhubungan langsung ke internet, maka komputer tersebut dapat berhubungan dengan komputer di belahan dunia manapun yang juga terhubung ke internet.

Sedangkan (Rafiudin, 2006) TCP/IP di definisikan koleksi (*suite*) protokol yang berperan dalam membangun environment jaringan global seperti internet. Protokol di referensikan pula sebagai suite protokol DoD (dee-oh-dee) atau *suite protokol Arpanet* karena mereka pada dasarnya di kembangkan oleh komunitas *riset advance research projects agency* (ARPA) dari *US department of defense* (DOD). Berikut ini lapisan yang ada pada *TCP/IP* :

1) Lapisan Fisik (*Physical Layer)*

Pada lapisan ini *TCP/IP* tidak di defenisikan protokol yang spesifik. Artinya *TCP/IP* Mendukung Semua Standar Dan *Proprietary* Protokol Lain.

2) Lapisan Jaringan Antarmuka (*Network Interface)*

Berfungsi untuk meletakkan frame – frame jaringan di atas media jaringan yang di gunakan. *TCP/IP* dapat bekerja dengan banyak teknologi transport, mulai dari teknologi *transport* dalam LAN (seperti halnya *Ethernet* dan

Token Ring), *MAN* dan *WAN* (seperti halnya *dial-up model* yang berjalan di atas *Public Switched Telephone Network* (PSTN), *Integrated Services Digital Network* (ISDN), serta *Asynchronous Transfer Mode* (ATM).

3) Lapisan Internet (*Internet Layer)*

Berfungsi untuk melakukan pemetaan (*routing*) dan enkapsulasi paket-paket data jaringan menjadi paket-paket IP. Protokol yang bekerja dalam lapisan ini adalah *Internet Protocol* (IP), *Address Resolution Protocol* (ARP), *Internet control Message Protocol* (ICMP), dan *Internet Group Management Protocol* (IGMP).

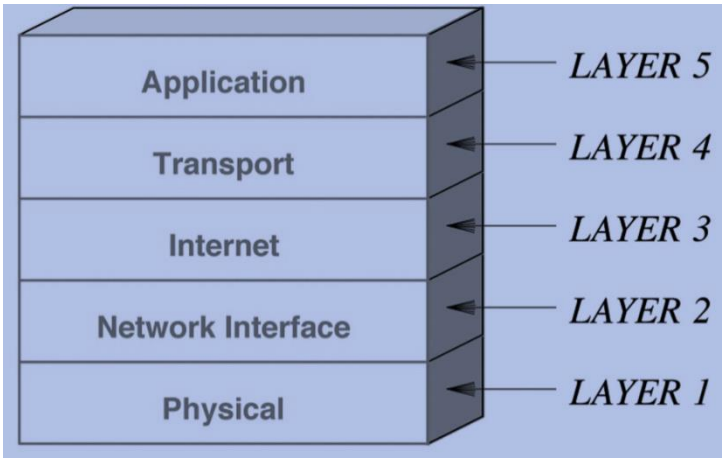
4) Lapisan Transport (*Transport Layer)*

Berguna untuk membuat komunikasi menggunakan sesi koneksi yang bersifat *connection-oriented* atau *broadcast* yang bersifat *connectionless*. Protokol dalam lapisan ini adalah *Transmission Control Protocol* (TCP) dan *User Diagram Protocol* (UDP).

5) Lapisan Aplikasi (*Application Layer)*

Merupakan Layer paling atas pada model *TCP/I*P, yang bertanggung jawab untuk menyediakan akses kepada aplikasi terhadap layanan *jaringan TCP/IP*. Protokol ini mencakup protokol *Dynamic* Host Configuration Protocol (DHCP), *Domain Name System* (DNS), *Hypertext Transfer Protocol* (HTTP), *File Transfer Protocol* (FTP), *Telnet, Simple Mail Transfer Protocol* (SMTP), *Simple Network Management Protocol* (SNMP), dan masih banyak protokol lainnya. Dalam beberapa implementasi *Stack Proto*col, seperti halnya *Microsoft*

TCP/IP, protokol-protokol lapisan aplikasi berinteraksi dengan menggunakan antarmuka *Windows Sockets* (Winsock) atau *NetBios over* TCP/IP (NetBT).



Gambar 2. 8TCP Reference Model

2.2.2. Line

Line adalah aplikasi instant messenger yang di luncurkan di Jepang sejak Juni 2011. Aplikasi LINE menggunakan sistem nomor telepon seluler penggunanya sebagai basis untuk saling berhubungan. Aplikasi Line saat ini tersedia untuk *gadget* yang memiliki sistem operasi *IOS* dan *Android* (No, Fauzan, Riadi, & Fadlil, 2016).

Aplikasi pesan instan atau *Instant Messaging* (IM) adalah suatu sistem pengiriman pesan dengan cepat melalui perantara jaringan internet dari satu komputer ke komputer lain dengan mengirim pesan dalam waktu nyata . Aplikasi *Instant Messaging* (IM) memiliki beberapa fungsi sebagai berikut:

1) Aplikasi *Instant Messaging* (IM) adalah media yang didesain untuk memperluas interaksi sosial manusia menggunakan internet dan aplikasi.

2) Aplikasi *Instant Messaging* (IM) mendukung demokratisasi pengetahuan dan informasi. Mentransformasi manusia dari pengguna isi pesan menjadi pembuat pesan itu sendiri.

Aplikasi *instant messaging* (IM) bernama *Line*, kini sedang naik daun. Aplikasi yang dirilis pada Juni 2011 ini telah diunduh setidaknya 300 juta kali dengan pengguna aktif dari 220 juta ditahun 2017. Aplikasi *LINE* menggunakan sistem nomor telepon seluler penggunanya sebagai basis untuk saling berhubungan. Aplikasi Line saat ini tersedia untuk perangkat yang memiliki sistem operasional *Ios, Android, Serta Windows.*

Aplikasi *Line* dapat diunduh secara gratis *di App Store* dan *Google Play*. LINE berbeda dari aplikasi *IM* lainnya, karena ada *emoticon* yang bervariasi. Ada Emoji yang menggambarkan kepala dengan bermacam ekspresi, lalu *Emoticons* berupa susunan karakter teks yang juga membentuk ekspresi, serta ada Stickers. Stickers ini yang cukup unik untuk Line, karena gambar ikonnya lucu-lucu, berukuran besar dan lebih ekspresif .

Naver, perusahaan asal Jepang yang mengembangkan aplikasi ini, melengkapi Line dengan beberapa aplikasi tambahan, yakni Line Camera dan Line Card untuk kartu ucapan. Pada awal April 2012, Naver memperluas penggunaan Line ke perangkat komputer. Line kini sudah tersedia untuk Mac dan Windows. Berkaitan dengan populernya aplikasi instant messenger, di dukung dengan adanya fitur-fitur yang menarik dan membantu proses komunikasi interpersonal lebih efektif. Di antara fitur instant messenger Line yang sering di gunakan adalah:

1) Personal Chat Fitur ini merupakan fitur utama yang diberikan oleh Line sebagai sarana komunikasi dengan pengguna Line lainnya secara private. Fitur personal chat ini pengguna Line dapat melakukan percakapan secara bebas tentang apa saja.
2) Share Foto atau Gambar Line memberikan fitur berbagai foto atau gambar baik secara personal melalui personal chat, ataupun melalui diskusi grup. Fitur ini memungkinkan pengguna memilih untuk mengambil gambar atau foto secara langsung dengan kamera ataupun mengambil dari galeri.
3) Free Call Free Call memungkinkan pengguna Line dapat menelpon pengguna Line lain dengan gratis karena menggunakan jaringan internet. Cara menggunakannya adalah dengan memilih teman yang ingin ditelepon lalu pilih ―Panggil‖.
4) Sticker Layaknya emoticon, sticker juga dapat digunakan untuk mengekspresikan sesuatu dengan bentuk dan gambar yang lebih besar, lebih lucu, dan lebih menarik.
5) Timeline Line menyediakan fitur timeline yang bisa digunakan untuk
6) Grup Line menyediakan fitur grup agar pengguna dapat berbincang-bincang dengan pengguna Line lebih dari satu pengguna .

Gambar 2. 9 Line Messenger

2.2.3. Network Forensic

Menurut (Kurniawan, 2012) Istilah *network forensic*s memang di ambil dari *terminology* yang berhubungan dengan *kriminologi*. *Network forensics* merupakan kegiatan untuk melakuakan pencarian data yang berhubungan dengan kejahatan di lingkungan jaringan komputer. Tantangan terberat dalam *network forensics* adalah memastikan keabsahan data dan memastikan dengan benar bahwa data yang di dapat memang berasal dari pengirimannya.

Kegiatan *network forensics* paling sering di lakukan ketika kejahatan pada jaringan komputer telah terjadi. Namun demikian, kegiatan analisis *network forensic* juga dapat di lakukan untuk menangkal atau mendeteksi kegiatan yang mungkin akan terjadi pada jaringan komputer.

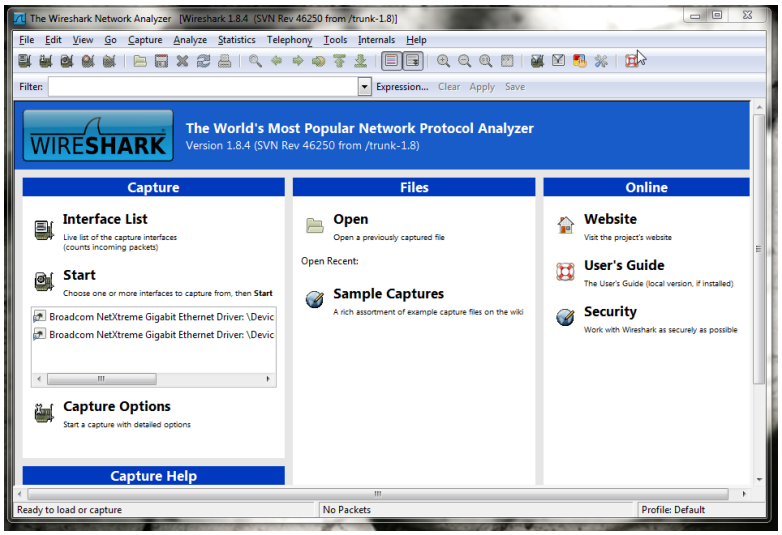
Network forensics bukanlah sebuah produk, namun proses yang cukup kompleks dimana kita dapat mengumpulkan data dan menganalisisnya, dan kemudian melakukan investigasi sesuai dengan kebutuhan. Ilmu network forensics sebenarnya adalah cabang ilmu baru yang merupakan bagian dari

digital *forensics*. ilmu ini berfokus pada analisis dan infestigasi data yang berasal dari paket jaringan.

2.3. Tool/software/aplikasi/*system*

2.3.1. Wireshark

Menurut (Kurniawan, 2012) Wireshark adalah tool yang di tujukan untuk penganalisisan paket data jaringan. Wireshark melakukan pengawasan paket secara waktu nyata (*real time)* dan kemudian menangkap data dan menampilkannya selengkap mungkin. Wireshark bisa di gunakan secara gratis karena aplikasi ini berbasis sumber terbuka. Aplikasi wireshark dapat berjalan di banyak di platform, seperti linux, windows, dan mac.



Gambar 2. 10 Line Messenger

Ada banyak hal yang dapat kita lakukan dengan wireshark. berikut ada beberapa contoh skenario yang mungkin menggambarkan kapan kita perlu menggunakan wireshark

1) Melakukan troubleshoot permasalahan jaringan.
2) Melakukan pengujian masalah jaringan.
3) Melakukan *debugging* implementasi protokol
4) Belajar protokol jaringan.

2.3.2. Fitur *Wirshark*

Wireshark dapat dikatakan sebagai *tools* analisis paket data jaringan yang paling sering digunakan. Berikut adalah sebagian fitur pada wireshark :

1. tersedia untuk platform unix, linux, windows, dan mac.
2. dapat melakukan capture paket data jaringan secara real time.
3. Dapat menampilkan informasi protokol secara lengkap.
4. Paket data dapat disimpan menjadi file dan nantinya dapat dibuka kembali.
5. Pemfilteran paket data jaringan.
6. Pencarian paket data dengan kriteria spesifik.
7. Pewarnaan penampilan paket data sehingga mempermudah penganalisisan data.
8. Menampilkan data statistik.

2.3.3. Protokol-Protokol Yang Paket Datanya Dapat Di Identifikasi Oleh Wireshark.

1) ARP (*Addres Resolution Protocol*) adalah protokol yang digunakan sebagai mekanisme untuk komunikasi mesin agar di kenal pada lingkungan jaringan tempat mesin itu berada. Teknik yang digunakan adalah memetakan alamat MAC dari *Ethernet* kealamat IP. Melalui protokol ini kita dapat mengetahui hubungan antara alamat MAC dan alamat IP.
2) ICMP (*Internet Control Message Protocol*) digunakan untuk menguji apakah suatu mesin dapat tercapai atau tidak, misalnya melakukan PING keportal google.com.
3) DHCP (*Dynamic Host Configuration Protocol*) digunakan sebagai protokol untuk mengatur pemberian alamat IP secara otomatis pada sebuah jaringan.
4) DNS (*Domain Name System*) adalah protokol yang sering digunakan untuk kebutuhan layanan di distribusi direktori pada internet.
5) IP (*internet protocol*) merupakan protokol layer jaringan pada model OSI yang berisi informasi mengenai alamat dan *control* yang memungkinkan paket data dirutekan.
6) TCP(*transmission control protocol*) yang berada pada layer transport pada model OSI dan menyediakan keandalan pengiriman paket secara stream dari layanan ke aplikasi dengan menarapkan beberapa mekanisme pengakuan pada kasus spesifik.

7) UDP (*user data protocol*) merupakan protocol berorientasi *connetionless* yang berada pada layer *transport* dari model OSI yang menawarkan kesederhanaan.
8) HTTP (*hypertext transfer protocol)* adalah protokol pada *application-level distributed, collaborative,dan hypermedia information system* .merupakan protokol yang sederhana untuk data raw yang melakukan transfer melintasi internet.

2.4. Penelitian Terdahulu

1. (Shade et al., 2014)**,** dengan judul artikel Analisis Rogue DHCP Packets Menggunakan Wireshark Network Protocol Analyzer, dalam jurnal Citec Journal**,** Vol. 2, No. 2, ISSN: 2354-5771(2015) dalam penelitian ini menjelaskan DHCP adalah protokol yang paling banyak digunakan di dunia, baik digunakan dalam jaringan kabel maupun nirkabel seperti pengelolaan jaringan warung internet, jaringan perkantoran, jaringan lab kampus, hotspot pada café atau sarana umum, jaringan antar ISP dan tethering atau portable hotspot pada smartphone. Di antara banyak keunggulan serta keuntungan yang ada, DHCP juga mempunyai beberapa kelemahan. Penggunaan DHCP di perlukan sebuah server untuk bertanggung jawab atas pemberian alamat IP kepada client, jika DHCP server mati maka seluruh client/ host dalam jaringan tersebut tidak terhubung satu sama lain karena

DHCP dibangun dengan sistem terpusat. Kelemahan lain dari protokol ini adalah adanya celah keamanan jaringan yang dapat di gunakan oleh network *attacker* untuk melakukan jenis serangan *man-in-the-middle* menggunakan *Rogue DHCP server*. *Rogue DHCP server* adalah *DHCP server* pada sebuah jaringan komputer yang tidak memiliki wewenang administratif atau bisa disebut server palsu yang di gunakan untuk melakukan serangan jaringan dengan menggunakan beberapa tools atau aplikasi di dalamnya terhadap server maupun client, sehingga DHCP server asli tidak dapat berfungsi secara optimal dalam memberikan layanan terhadap client. Rogue DHCP server di dalam sebuah jaringan akan merusak sistem keamanan dan menimbulkan masalah privasi bagi client yang dapat menciptakan serangan jahat seperti sniffing lalu-lintas jaringan, serangan masquerading, dan serangan DOS. Hal ini dapat digunakan oleh para penyerang untuk mengarahkan dan mengintersepsi lalu lintas jaringan dari perangkat apapun yang tergabung dalam jaringan DHCP sehingga penyerang menjadi man-in-the-middle yang dapat melihat dan memodifikasi isi asli dari komunikasi Penelitian dilakukan untuk mengetahui bagaimana proses pertukaran paket DHCP beserta parameter yang terkandung di dalamnya, sebelum adanya Rogue DHCP server, setelah adanya Rogue DHCP server, dan setelah adanya pencegahan terhadap Rogue DHCP server di dalam jaringan DHCP berbasis IPv4. Skenario penelitian dibuat dengan DHCP server asli dibangun di dalam intermediate device berupa bridge mikrotik, 2 buah

client menggunakan Windows XP, dan 1 client menggunakan linux backtrack yang difungsikan sebagai Rogue DHCP server menggunakan mesin virtual VMware workstation. Analisis difokuskan pada pengamatan paket DHCP beserta parameter yang ada di dalamnya menggunakan wireshark network protocol analyzer yang bertujuan untuk menciptakan sistem kemanan jaringan berupa monitoring dan pencegahan terhadap Rogue DHCP server dengan menggunkan fitur yang ada pada mikrotik yaitu DHCP alert yang dikombinasikan dengan Firewall filter. Tujuan dari penelitian ini dimaksudkan untuk menganalisis Rogue DHCP packets yang disebarkan oleh Rogue DHCP server di dalam jaringan DHCP, serta memberikan solusi pencegahan dan monitoring pada intermediate device yang menghubungkan antara DHCP server dengan DHCP client terhadap Rogue DHCP server di dalam jaringan DHCP, dengan hasil akhir penelitian dapat digunakan sebagai acuan dalam penerapan sistem keamanan jaringan DHCP terhadap Rogue DHCP server serta dapat sebagai referensi untuk pengembangan fitur pada perangkat jaringan intermediate device berupa switch atau bridge dalam pencegahan Rogue DHCP server.

2. (Dewi, 2012), dengan judul artikel Analisis Komunikasi Data Pada Aplikasi Percakapan Suara Menggunakan Perangkat Lunak Wireshark, dalam jurnal POLI REKAYASA Volume 8, Nomor 1, ISSN : 1858-3709 (2012).dalam penelitian ini menjelaskan Saat ini, di semua lapisan dunia perkembangan teknologi sangatlah pesat sekali. Terutama dibidang

telekomunikasi dan jaringan komputer. Berbagai macam model alat komunikasi dapat dijumpai, baik yang berupa fisik (hardware) ataupun berupa aplikasi (software). Salah satu aplikasi yang paling sering digunakan untuk bertukar informasi adalah aplikasi percakapan (chatting), baik berupa text, suara ataupun video. Dengan aplikasi ini, siapa saja dibelahan bumi ini dapat berkomunikasi, hanya dengan bermodalkan akses internet. agar proses ini dapat berlangsung pada masing-masing komputer harus dilakukan beberapa proses. Yaitu, melakukan pendaftaran dengan alamat IP address (internet protocol address), yang dibutuhkan untuk proses pelaksanaan percakapan antar user/client. Aplikasi ini dibuat menggunakan bahasa pemrograman Visual Basic 6.0 (VB 6.0) dan dilengkapi dengan basis data menggunakan Microsoft Access 2007 Adapun permasalahan yang dibahas dalam penelitian ini adalah lebih menitikberatkan pada bagaimana memanfaatkan perangkat lunak wireshark untuk menganalisis proses komunikasi data pada aplikasi percakapan suara yang berbasis jaringan LAN. Disamping itu juga membahas sedikit tentang bagaimana membuat program aplikasi percakapan suara ini menggunakan bahasa pemrograman Visual Basic 6.0.

3. (Widodo, 2013)Dengan judul Pemantauan Jaringan Komputer dengan DNS Server Berbasis Routing StatisMenggunakan Wireshark ISSN : 2252-4908 Vol. 1 No. 2 Agustus 2012 dalam penelitian ini menjelaskan Membangun suatu jaringan komputer dibutuhkan beberapa tahapan, mulai dari perencanaan, perancangan, implementasi, dan pengujian. Selanjutnya

adalah kegiatan perawatan sampai dengan proses pemantauan. Pada tahap perancangan perlu diperhatikan tingkat kompleksitas jaringan, permasalahan *collision domain* dan *broadcast domain* yang dapat mengganggu kinerja jaringan komputer. Sebuah *collision domain* bagian dari jaringan dimana data paket dapat berbenturan dengan satu sama lain ketika dikirim pada suatu media bersama ketika menggunakan ethernet. Sebuah tabrakan jaringan terjadi ketika lebih dari satu perangkat berusaha mengirim paket pada segemen jaringan pada saat yang sama. Jaringan kabel menggunakan switch untuk menghubungkan setiap perangkat langsung ke port pada switch. *Broadcast domain* adalah sebuah divisi logis dari sebuah jaringan komputer, dimana semua node dapat mencapai satu sama lain dengan broadcast pada lapisan data link. Sebuah *broadcast domain* dapat berada dalam segmen jaringan komputer yang sama ataupun berbeda. Perbedaan antara *broadcast domain* dan *collision domain* itu muncul karena sistem Ethernet menggunakan sistem bersama. Dalam Ethernet sederhana, frame data dikirimkan ke semua node lain pada jaringan. Setiap node menerima, memeriksa alamat tujuan dari setiap frame. *Broadcast domain* dapat dipisahkan oleh perangkat yang bekerja pada layer 3 (*network layer*) seperti router dan switch layer 3 Hubungan antara *collision domain* dan *broadcast domain* .

4. (Yuvandra & Zulfin, n.d.) dengan judul ANALISIS KINERJA TRAFIK *VIDEO CHATTING* PADA SISTEM *CLIENT-CLIENT* DENGAN APLIKASI *WIRESHARK* dalam jurnal issn : VOL. 3 NO. 3/September

2013 dalam penelitian ini menjelaskan Perkembangan di era yang berbasis *internet* sekarang ini, perkembangan kemajuan teknologi pada dunia telekomunikasi juga semakin pesat, diantaranya adalah *video chatting*, karena orangorang yang berada di tempat lain yang jauh dan ingin berkomunikasi dengan orang yang berada di tempat lain yang jauh pula. *Video chatting* dapat digunakan sebagai alat yang dapat menyalurkan gambar serta suara dalam bentuk video sehingga terlihat seperti nyata. Caranya, hanya dibutuhkan *webcam*, *monitor*, *speaker*, *mikrofon*, yang dewasa ini terintegrasi dalam satu *gadget* yaitu laptop. Salah satu contoh aplikasi *video chatting* adalah *skype*. *Skype* adalah *software* aplikasi komunikasi suara berbasis IP melalui *internet* antara sesama pengguna *skype*. Pada saat kedua pengguna skype sudah terhubung melalui internet dan mulai melakukan *chatting*, maka akan mengakibatkan trafik di jaringan internet tersebut semakin meninggi, sehingga penulis ingin memonitoring trafik di jaringan internet tersebut dengan menggunakan *software wireshark.* W*ireshark* dapat menangkap semua trafik saat pemakai menggunakan jaringan internet, baik *ip address*, *protocol*, maupun informasi di dalam paket data itu sendiri. Pada tulisan ini membahas tentang analisis kinerja trafik *video chat* berdasarkan lamanya waktu melakukan *chatting* di jaringan internet. Parameter yang akan dianalisis adalah *delay*, *throughput* dan *packet loss* yang dihasilkan pada waktu terjadi pengiriman paket data dari *request* (permintaan) sampai *receive* (menerima) dari sisi suatu *client* dengan *client* lain yang akan

dituju sampai keduanya mengakhiri *chatting*nya.

5. Case, P., & Engineering, C. (2014). SIGNATURE BASED PACKET SNIFFER, *7782*, 155–158.Packet sniffer is a program running in a network attached Device that passively receives all data link layer frames passing through the device’s network adapter. It is also known as Network or Protocol Analyzer or Ethernet Sniffer. The packet sniffer captures the data that is addressed to other machines, saving it for later analysis. It can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic. Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission. This is unlike standard network hosts that only receive traffic sent specifically to them. The security threat presented by sniffers is their ability to capture all incoming and outgoing traffic, including clear-text passwords and usernames or other sensitive material. Each machine on a local network has its own hardware address which differs from other machines'. When a packet is sent, it will be transmitted to all available machines on local network. Owing to the shared principle of Ethernet, all computers on a local network share the same wire, so in normal situation, all machines on network can see the traffic passing through but will be unresponsive to those packets do not belong to themselves by just ignoring. However, if the network interface of a machine is in promiscuous mode, the NIC of this machine can take over all packets and

a frame it receives on network, namely this machine (involving its software) is a sniffer [1]. When a packet is received by a NIC, it first compares the MAC address of the packet to its own. If the MAC address matches, it accepts the packet otherwise filters it. This is due to the network card discarding all the packets that do not contain its own MAC address, an operation mode called no promiscuous, which basically means that each network card is minding its own business and reading only the frames directed to it. In order to capture the packets, NIC has to be set in the promiscuous mode. Packet sniffers which do sniffing by setting the NIC card of its own system to promiscuous mode, and hence receives all packets even they are not intended for it. So, packet sniffer captures the packets by setting the NIC card into promiscuous mode the packet arriving at the NIC are copied to the device driver memory, which is then passed to the kernel.The internet is an essential part of our everyday life and many imperative and crucial services like banking, shopping, transport, health, and communication are partly or completely dependent on the internet. To tenacitynetwork traffic used Wireshark tool. Development and evaluation of protocols and algorithms for these fields requires answering many design questions. Although small-scale evaluation in a lab, wide-area test beds, and custom simulators can all be valuable, each has significant short-comings. These approaches often lack the wide mix of circulation and topologies found in real networks Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software

and communications protocol development, and education.it runs on Linux, OS X, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.Wireshark is a network packet analyzer. A network packet analyzer will try to arrest network packets and tries to display that packet data as detailed as possible. Wireshark is perhaps one of the best open source packet analyzers available today. When you launch Wireshark, choose which interface you want to bind to and click the green shark fin icon to get going. Packets will instantly start to be captured. Once you've collected what you need, you can disseminate the data to a file for analysis in another application or use the in-built filter to drill down and analyze the captured packets at a deeper level from within Wireshark itself. Wireshark Network Analysis, gives a light-hearted yet serious list of ways in which this open source network analysis tool can help any network analyst become better at his or her job.

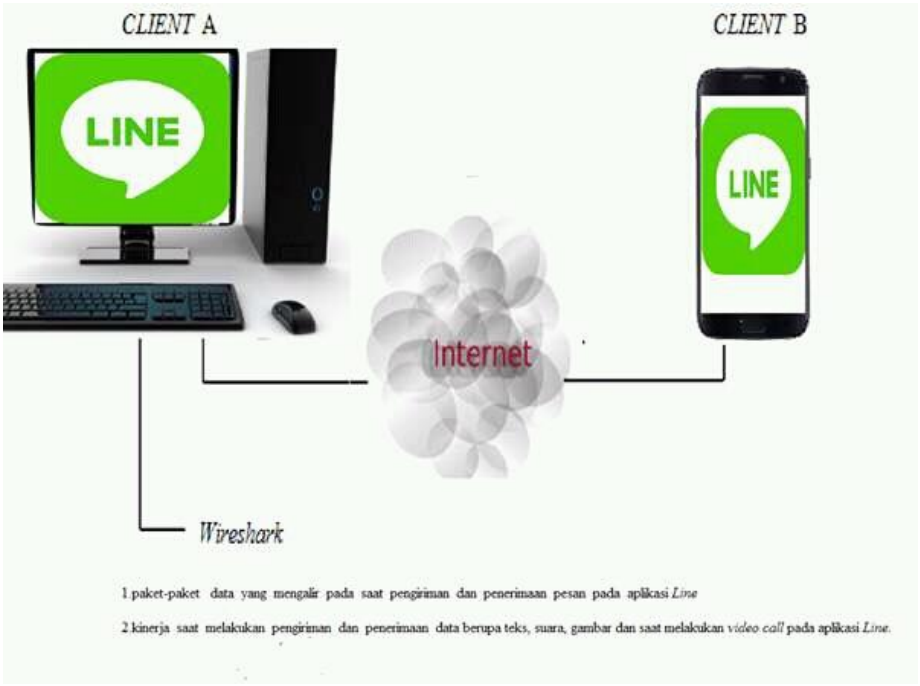
6. Devi, M. (2016). " INVESTIGATINGAND ANALYSIS OF NETWORK TRAFFIC USING WIRESHARK TOOL ," *3*, 26–33. The internet is an essential part of our everyday life and many imperative and crucial services like banking, shopping, transport, health, and communication are partly or completely dependent on the internet. To tenacitynetwork traffic used Wireshark tool. Development and evaluation of protocols and

algorithms for these fields requires answering many design questions. Although small-scale evaluation in a lab, wide-area test beds, and custom simulators can all be valuable, each has significant short- comings. These approaches often lack the wide mix of circulation and topologies found in real networks Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.it runs on Linux, OS X, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.Wireshark is a network packet analyzer. A network packet analyzer will try to arrest network packets and tries to display that packet data as detailed as possible. Wireshark is perhaps one of the best open source packet analyzers available today. When you launch Wireshark, choose which interface you want to bind to and click the green shark fin icon to get going. Packets will instantly start to be captured. Once you've collected what you need, you can disseminate the data to a file for analysis in another application or use the in-built filter to drill down and analyze the captured packets at a deeper level from within Wireshark itself. Wireshark Network Analysis, gives a light-hearted yet serious list of ways in which this open source network analysis tool can help any network analyst become better at his or her job.

2.5.Kerangka pemikiran

Kerangka berfikir merupakan model konseptual tentang bagaimana teori berhubungan dengan berbagai faktor yang telah diidentifikasi sebagai masalah yang penting. Kerangka berfikir yang baik akan menjelaskan secara teoritis pertautan antara variabel yang akan diteliti. Seorang peneliti harus menguasai teori-teori ilmiah sebagai dasar bagi argumentasi dalam menyusun kerangka pemikiran yang membuahkan hipotesis(Sugiyono, 2014).

Untuk memudahkan dalam penelitian, peneliti menyusun alur kerangka pemikiran sebagai berikut :



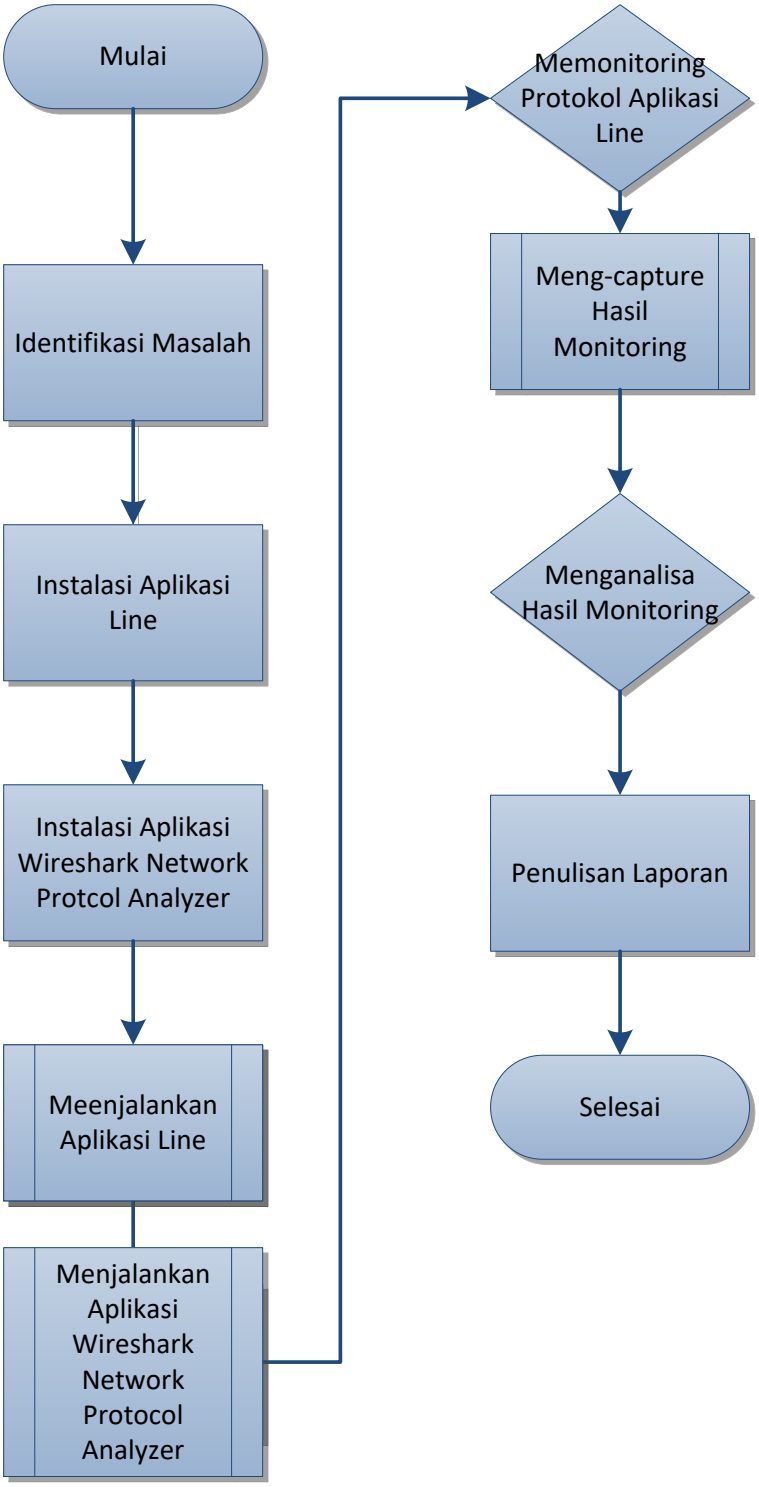
Gambar 2. 11 Kerangka Pemikiran

BAB III

METODE PENELITIAN

3.1. Desain Penelitian

Penelitian sebagai metode ilmiah adalah cara untuk mencari dan mengungkapkan kebenaran dengan ciri objektivitas. Di sini kebenaran yang di peroleh secara konseptual dan dedukti saja tidak cukup. Oleh karena itu, kebenaran juga harus tetap di uji secara empiris. Secara umum penelitian di artikan sebagai proses pengumpulan dan analisis data yang di lakukan secara sistematis dan logis untuk mencapai tujuan-tujuan tertentu. Pengumpulan dan analisis data itu menggunakan metode-metode ilmiah, baik yang besifat kuantitatif maupun kualitatif, eksperimental maupun non eksperimental, interaktif maupun non interktif. Metode penelitian atau metodologi penelitian yang dalam makna lebih luas merupakan desain atau rancangan penelitian. Rancangan ini berisi rumusan tentang objek atau subjek yang di teliti, teknik- teknik pengumpulan data, serta prosedur pengumpulan dan analisis data berkenaan dengan fokus masalah tersebut. Adapun rancangan penelitian dapat di lihat sebagai berikut :


Mulai
Identifikasi Masalah
Instalasi Aplikasi Line
Instalasi Aplikasi Wireshark Network Protcol Analyzer
Meenjalankan Aplikasi Line
Menjalankan Aplikasi Wireshark Network Protocol Analyzer
Memonitoring Protokol Aplikasi Line
Meng-capture Hasil Monitoring
Menganalisa Hasil Monitoring
Penulisan Laporan
Selesai

Gambar 3. 1 Desain Penelitian

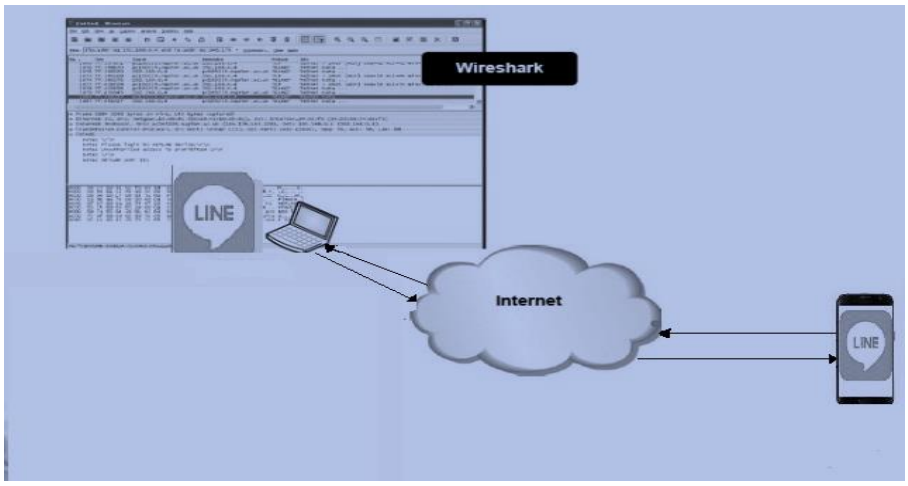
3.2. Operasional Variabel Penelitian

Data penelitian berupa pengamatan atau observasi langsung di dapatkan dari variabel-variabel parameter. dari variabel lalu lintas pada aplikasi line yang akan dianalisis menjadi sebuah acuan yaitu terdiri dari :

1) Paket data saat mengirim pesan.
2) Paket data saat menerima pesan.

3.3. Objek Monitoring

Objek monitoring dalam penelitian ini adalah segala sesuatu yang akan dijadikan subjek atau objek penelitian yang dikehendaki oleh peneliti. Maka yang akan dijadikan objek dalam melakukan penelitian ini seperti:



Gambar 3. 2 Objek Monitoring

Kedua perangkat akan melakukan aktivitas diinstan messenger Line. Peneliti akan memonitoring protokol yang ada di aplikasi line . Penelitian ini dilakukan menggunakan menggunakan laptop yang sudah terpasang aplikasi Line, dan juga wireshark.

3.4. Teknik Dan Alat Pengumpulan Data

-

3.4.1. Teknik Pengumpulan Data

Metode pengumpulan data adalah cara atau teknik yang dapat digunakan oleh peneliti untuk mengumpulkan data .metode (cara atau teknik) menunjukkan suatu kata yang abstrak dan tidak diwujudkan dalam benda sehingga hanya penggunaannyaa saja yang bisa di perlihatkan. Pengumpulan data dalam penelitian dimasudkan untuk memperoleh bahan, keterangan, kenyataan, dan informasi yang dapat dipercaya. Untuk memperoleh data seperti yang dimaksudkan, dalam penelitian saat digunakan berbagai macam metode, di antaranya angket, pengamatan, wawancara, tes, analisis, dokumen, dan sebagainya. Peneliti saat menggunakan salah satu atau gabungannya tergantung pada masalah yang dihadapi.

3.4.2. Pengamatan Atau Observasi

Pengamatan atau observasi adalah suatu teknik atau cara untuk mengumpulkan data dengan cara meengamati kegiatan yang sedang

berlangsung. Pengamatan dapat dilakukan dengan partisipasi maupun nonpartisipasi. Dalam pengamatan dapat dilakukan dengan partisipatori (participatory observasion) pengamat ikut serta dalam kegiatan yang sedang berlangsung. Pengamat ikut sebagai peserta pelatihan sementara dalam pengamatan nonpartisipatori (nonparticipatory observasion) pengamat tidak serta dalam kegiatan, pengamat hanya berperan dalam mengamati kegiatan. observasi terbagi dalam beberapa jenis, sebagai berikut :

1) Observasi Partisipatif

   Dalam observasi ini, peneliti terlibat dengan kegiatan sehari-hari orang yang sedang diamati atau yang digunakan sebagai sumber data penelitian.

2) Obserasi Terus Terang Atau Tersemar

   Dalam hal ini, peneliti dalam melakukan pengumpulan data menyatakan terus terang kepada sumber data, bahwa ia sedang melakukan penelitian.

3) Observasi Terstruktur

   Obeservasi dalam penelitian kualitatif dilakukan dengan tidak berstruktur, karena fokus peneitian belum jelas. Fokus observasi akan berkembang selama kegiatan observasi berlangsung. Kalau masalah penelitian sudah jelas seperti dalam penelitian kualitatif, maka observasi dapat dilakukan secara berstruktur dengan menggunakan pedoman observasi.

3.4.3. Dokumentasi

Dokumentasi di tujukan untuk memperoleh data langsung dari tempat penelitian, meliputi bukti, peraturan, laporaan kegiatan, foto, film dokumenter, dan data yang relevan dengan penelitian. Dokumentasi merupakan catatan peristiwa yang sudah berlalu. Dokumen biasanya berbentuk tulisan, gambar, atau karya monumental seseorang.

3.5. Alat Pengumpulaan Data

Berikut uraian yang di gunakan sebagai alat pengumpulana data protokol pada aplikasi line :

Tabel 3. 1 Alat Pengumpulan Data

No.	Alat Pengumpulan Data	Pengertian	Spesifikasi	Kegunaan
1	Laptop Asus X453MA	Komputer portable yang sumber dayanya berasal dari baterai	· Windows Edition : Windows 10 Pro · Intel(R) Celeron(R) CPU N2930 @ 1.83GHz (4 CPUs), ~1.8GHz · Ram : 4.00 Gb · System Type : 64-Bit Operating System, x64-Based Processor	sebagai wadah dalam dalam melakukan penelitian.
2	Aplikasi Line	Aplikasi pengirim pesan instan gratis yang dapat digunakan pada berbagai platform seperti smartphone, tablet, dan komputer.	Ver. 5.2.2.1459	protokol pada aplikasi ini yang akan dianalisis
3	Aplikasi Wireshark Network Protocol Analyzer	tool yang ditujukan untuk penganalisisan paket data jaringan	Version 2.2.6 (v2.2.6-0-g32dac6a)Compiled (64-bit) with Qt 5.6.1, with WinPcap (4_1_3)	aplikasi yang digunakan untuk memonitoring
4	Tab Asus fonepad 7	tablet juga merupan komputer portable yang seluruhnya berupa layar sentuh	• GSM / HSPA 2G, 3G • SPEED HSDPA 850/900/1900/2100 • OS ANDROID 4.3 (JELLY BEAN) • INTEL ATOM Z2520 DUAL-CORE 1.2 GHZ	sebagai user 2 aplikasi line

3.6. Jadwal Penelitian

jadwal penelitian yang di lakukan oleh peneliti di uraikan sebagai berikut :

3.6.1. Jadwal Penelitian

Jadwal penelitian di susun mulai dari pengumpulan judul, tahap-tahap penelitian, hingga pengumpulan skripsi. Jadwal penelitian ditampilkan pada tabel 3.3. seperti berikut :

Tabel 3. 2 Jadwal Penelitian

Tahapan Kegiatan	Waktu Penelitian 2016/2017																			
	Mar-17			Apr-17			Mei-17			Jun-17			Jul-17			Agu-17			Sep-17		
Pengajuan Judul																				
BAB I																				
BAB II																				
BAB III																				
BAB IV																				
BAB V																				
Penyerahan Soft Copy																				