LAPORAN PRAKTEK KERJA LAPANGAN

APLIKASI PACKET SNIFFER DENGAN BAHASA PYTHON

Oleh:
I PUTU KUSWARA ADI PRADANA
NIM : 1308605017

Pembimbing:
I Dewa Made Bayu Atmaja Darmawan, S.Kom., M.Cs.

Program Studi Teknik Informatika
Jurusan Ilmu Komputer
Fakultas Matematika Dan Ilmu Pengetahuan Alam
Universitas Udayana
2016

HALAMAN PENGESAHAN

APLIKASI PACKET SNIFFER DENGAN BAHASA PYTHON

Oleh:
I Putu Kuswara Adi Pradana
NIM : 1308605017

Bukit Jimbaran, 8 Desember 2016
Menyetujui,

Dosen Pembimbing	Pembimbing Lapangan
I Dewa Made Bayu Atmaja Darmawan, S.Kom., M.Cs.	I Gede Oka Gatria Atitama, S.Kom., M.Kom.
NIP. 198901272012121001	NIP. 199102262016031200 1

Mengetahui,
Ketua Jurusan Ilmu Komputer
FMIPA Universitas Udayana

Agus Muliantara, S.Kom., M.Kom.
NIP. 198006162005011001

KATA PENGANTAR

Puji dan syukur dipanjatkan kehadirat Tuhan Yang Maha Esa karena atas segala berkat dan karunia-Nya sehingga dapat terselesaikannya laporan praktek kerja lapangan (PKL) dengan judul "Aplikasi Packet Sniffer Dengan Bahasa Python".

1. Bapak Agus Muliantara, S.Kom., M.Kom. selaku ketua Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Udayana
2. Bapak I Dewa Made Bayu Atmaja Darmawan, S.Kom., M.Cs. selaku pembimbing yang telah memberikan bimbingan, arahan, dan masukan selama penyusunan laporan ini.
3. Semua rekan – rekan Praktek Kerja Lapangan di lingkungan Jurusan Ilmu Komputer yang mendukung dan memberikan saran – saran kepada penulis selama melakukan Praktek Kerja Lapangan
4. Semua pihak yang telah membantu hingga laporan ini dapat terselesaikan.

Disebabkan keterbatasan pengetahuan dan kemampuan yang dimiliki, menyadari laporan ini jauh dari sempurna. Kritik dan saran yang bersifat membangun sangat diharapkan dari pembaca.

Akhir kata terima kasih dan mohon maaf apabila terdapat kesalahan baik yang disengaja maupun tidak disengaja.

Jimbaran, 1 Desember 2016

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Traffic yang ada pada jaringan perlu diawasi untuk memudahkan admin dalam control atau mencegah terjadinya kegagalan dalam jaringan. Penggunaan jaringan internet bervariasi, seperti download file, streaming, browsing dan lain-lain. Disisi lain bandwidth yang dimiliki terbatas. Oleh karena itu, dibutuhkan pengaturan yang baik untuk menggunakan bandwidth yang terbatas itu. Pada tulisan ini akan dibahas bagaimana sistem aplikasi yang dapat memonitor atau memberikan laporan dari lalu lintas paket data dalam jaringan komputer sehingga dapat menjadi informasi bagi seorang admin untuk menerapkan kebijakan-kebijakan penganturan bandwidth.

Aplikasi dikembangkan dengan bahasa pemrograman python berbasis desktop. Bahasa pemrograman python mendukung banyak library, sehingga pengembangan aplikasi menjadi lebih mudah. Data hasil pelaporan meliputi alamat IP sumber, alamat IP tujuan, alamat IP yang paling sering dituju, maupun jumlah packet data yang menuju ke suatu alamat IP tertentu.

Aplikasi yang dikembangkan diharapkan dapat digunakan oleh seorang admin dalam mendapatkan informasi mengenai lalu lintas data yang sedang berjalan pada jaringan komputer yang dikelolanya. Informasi ini tentu saja diharapkan sebagai masukan yang dapat dipahami dengan mudah oleh admin. Informasi-informasi tersebut dapat digunakan dalam memblokir suatu alamat IP atau mengurangi traffic bandwidth ke suatu alamat IP, atau mungkin dapat membuat kebijakan-kebijakan dalam sisi firewall atau sisi keamanan tingkat atas berdasarkan informasi yang diberikan oleh sistem yang dibangun, sehingga admin dengan cepat dapat membuat kebijakan dalam mengelola bandwidth yang dimiliknya.

1.2 Tujuan

Adapun tujuan yang ingin dicapai dalam pembuatan aplikasi paket snifer dengan bahasa python adalah sebagai berikut :

1. Membantu administrator server dalam mengatahui lalu lintas paket data yang sedang berlangsung.
2. Membantu administrator server dalam membuat kebijakan-kebijakan lalu lintas data berdasarkan hasil aplikasi packet sniffer.

1.3 Manfaat

Adapun tujuan yang ingin dicapai dalam pembuatan aplikasi paket snifer dengan bahasa python adalah sebagai berikut :

1.3.1 Manfaat Bagi Penulis

Beberapa manfaat yang diperoleh penulis dalam pembuatan aplikasi sniffer adalah :

1. Menyesuaikan diri dalam menghdapai lingkungan kerja setelah menyelesaikan studi
2. Melihat secara langsung penggunaan / penerapan teknologi dan komunikasi di tempat praktek kerja

1.2.2 Manfaat Bagi Instansi PKL

Beberapa manfaat yang didapatkan bagi instansi dari adanya program packet sniffer adalah :

1. Membantu memberikan data mengenai paket data untuk digunakan dalam kebijakan-kebijakan pada firewall dan lalu lintas data pada instansi.

1.4 Waktu dan Tempat Pelaksanaan

Pelaksanaan praktek kerja lapangan bertempat di Jurusan Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana, di Jalan Kampus Bukit Jimbaran. Dimulai pada tanggal 1 Maret 2016 sampai dengan XX XXXX 2016, yaitu selama 3 bulan. Pelaksanaan jam praktek kerja lapangan disesuaikan dengan jam kuliah di Jurusan Ilmu Komputer, FMIPA, Unud yaitu pukul 08.30 wita – 16.00 wita.

BAB II
GAMBARAN UMUM

2.1 Sejarah Jurusan Ilmu Komputer

Ilmu Komputer merupakan ilmu terapan dari ilmu – ilmu dasar yang mengalami perkembangan sangat pesat seiring dengan pesatnya perkembangan Ilmu Pengetahuan dan Teknologi (IPTEK). Penguasaan bidang ilmu komputer belakangan ini sangatlah dirasa perlu dalam meningkatkan sumber daya manusia sebagai tuntutan dari perkembangan teknologi. Khususnya dalam mendukung peningkatan kualitas Tri Dharma Pergurusan Tinggi di dalam institusi dan untuk menunjang proses – proses pembangunan masyarakat (daerah dan nasional), bidang ilmu komputer sengat dirasa perlu dikembangkan di Universitas Udayana (Unud).

Gejala meningkatnya kebutuhan terhadap tenaga – tenaga terdidik, terampil, dan profesional di bidang ilmu komputer dan terapannya telah diantisipasi oleh pimpinan Unud sejak tahun 2005. Berawal dari persetujuan Senat Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Udayana (FMIPA Unud) tanggal 13 Agustus 2005 tentang Pembentukan Program Studi Ilmu komputer di Fakultas MIPA Unud yang kemudian dilanjutkan ketingkat Universitas melalui persetujuan Rapat Pimpinan Universitas Udayana tanggal 15 September 2005 yang menyetujui pendirian Jurusan Ilmu Komputer di Fakultas MIPA Unud.

Seiring dengan perjalanan waktu, akhirnya pada tanggal 12 April 2006 dikeluarkanlah Ijin Penyelenggaraan PS Ilmu komputer dari DIRJEN DIKTI dengan Surat Keputusan DIKTI No.1193/D/T/ 2006 yang berlaku selama 2 tahun terhitung dari tahun pertama akademik, maka Jurusan/PS Ilmu komputer FMIPA Unud secara resmi menyelenggarakan perkuliahan untuk mahasiswa angkatan I (tahun akademik 2006/2007) pada tanggal 3 September 2006 dengan jumlah

mahasiswa terdaftar 100 (seratus) orang dari kapasitas sebenarnya yang hanya 50 (lima puluh) orang. Animo masyarakat untuk mendalami bidang ilmu komputer memang sangat tinggi, hal ini dapat dilihat dari banyaknya pendaftar pada angkatan pertama sebanyak 291 orang.

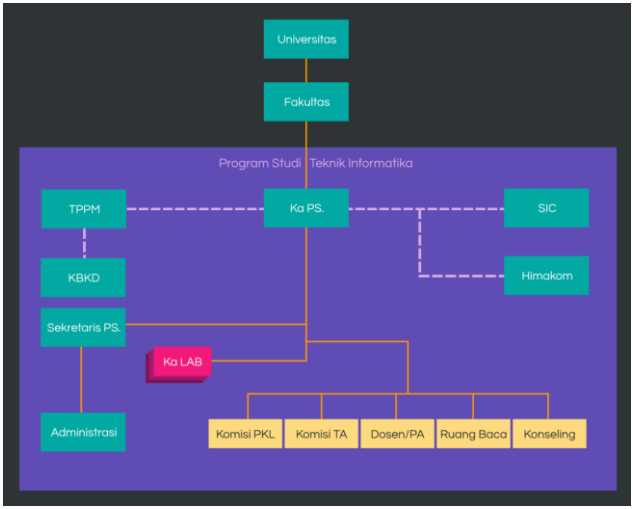
Begitu juga pada tahun ajaran 2007/2008 dimana Jurusan Ilmu Komputer sebagai jurusan baru sudah dapat mensejajarkan diri dengan jurusan - jurusan favorit lainnya dalam penerimaan mahasiswa dengan masuknya Jurusan Ilmu Komputer sebagai salah satu jurusan yang memperolah mahasiswa sesuai dengan kuota peneriamaan sehingga tidak ada bangku kosong.

2.2 Kegiatan Jurusan Ilmu Komputer

Jurusan Ilmu Komputer merupakan salah satu jurusan yang berada di bawah naungan Fakultas Matematika dan Ilmu Pengetahuan Alam, Unviersitas Udayana, yang memiliki beberapa aktivtias – aktivitas akademik maupun non akademik, yaitu antara lain: belajar mengajar, seminar publikasi ilmiah, pengabdian masyarakat, kegiatan organisasi mahasiswa (Himakom dan SIC), dan lain sebagainya.

2.3 Struktur Kepengurusan Jurusan Ilmu Komputer

Jurusan Ilmu Komputer, FMIPA Unud memiliki struktur kepengurusan sebagai berikut



2.4 Visi, Misi, dan Tujuan Jurusan Ilmu Komputer

Karakteristik Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Udayana saat sangat dipengaruhi oleh kekuatan serta kelemahan internal jurusan serta peluang dan ancaman yang terdapat pada eksternal sistem. Karakter jurusan yang hendak dibangun juga akan ditentukan oleh visi, misi, dan tujuan pendidikan yang hendak dikembangkan. Untuk itu, akan diuraikan visi, misi, serta tujuan pendidikan yang menjadi penciri karakteristik Jurusan Ilmu Komputer FMIPA UNUD.

2.4.1 Visi Jurusan Ilmu Komputer

Menjadi Program Studi yang unggul dan mampu menciptakan lulusan yang mandiri serta berbudaya dalam pengembangan teknologi informasi di tingkat nasional dan internasional.

2.4.2 Misi Jurusan Ilmu Komputer

Adapun Misi Jurusan Ilmu Komputer Fakultas MIPA Universitas Udayana dapat dijabarkan sebagai berikut:

a. Menyelenggarakan dan mengorganisasikan pendidikan yang adaptif dan responsif pada kebutuhan pembangunan nasional dan internasional.
b. Mengembangkan penelitian dan pengabdian kepada masyarakat sehingga mampu mengatasi permasalahan-permasalahan nyata dibidang teknologi informasi.
c. Menciptakan lulusan yang berkualitas, madri, profesional dan berbudaya dalam pengembangan teknologi informasi sesuai dengan norma dan etika yang berlaku.

2.4.3 Tujuan Jurusan Ilmu Komputer

Tujuan Jurusan Ilmu Komputer Fakultas MIPA Universitas Udayana dapat dijabarkan sebagai berikut:

a. Mengembangkan kurikulum adaptif dan responsif terhadap tuntutan pembangunan nasional dan internasional.
b. Mengembangkan kemampuan civitas akademika dalam mendukung terwujudnya proses pendidikan yang berkualitas dan efisien.
c. Meningkatkan kuantitas dan kualitas penelitian yang dilakukan oleh dosen dan mahasiswa yang bermanfaat untuk pengembangan pendidikan dan pengabdian kepada masyarakat

BAB III
KAJIAN PUSTAKA

3.1 Paket Data Jaringan

Paket data jaringan atau network packet adalah satuan informasi dasar yang dapat ditransmisikan di atas jaringan atau melalui saluran komunikasi digital. Sebuah paket berisi packet header yang berisi informasi mengenai protokol tersebut (informasi mengenai jenis, sumber, tujuan, atau informasi lainnya), data yang hendak ditransmisikan yang disebut dengan data payload, dan packet trailer yang bersifat opsional. Sebuah paket memiliki struktur logis yang dibentuk oleh protokol yang digunakannya. Ukuran setiap paket juga dapat bervariasi, tergantung struktur yang dibentuk oleh arsitektur jaringan yang digunakan. Paket jaringan juga dapat disebut datagram, frame, atau cell.

3.2 TCP/IP

3.2.1. Pengertian TCP/IP

TCP/IP adalah sekumpulan protokol yang terdapat didalam jaringan komputer (network) yang digunakan untuk berkomunikasi atau bertukar data antar komputer. TCP/IP merupakan protokol standar pada jaringan internet yang menghubungkan banyak komputer yang berbeda jenis mesin maupun sistem operasi agar dapat berinteraksi satu sama lain (Melwin Syafrizal, 2005:96).

Protokol merupakan himpunan aturan yang memungkinkan komputer untuk berhubungan antara satu dengan yang lain, biasanya berupa bentuk waktu, barisan, pemeriksaan error saat transmisi data.

Komputer yang terhubung ke internet berkomunikasi dengan protokol ini. Karena menggunakan bahasa yang sama, yaitu protokol TCP/IP, perbedaan jenis komputer dan sistem operasi tidak menjadi masalah. Komputer PC dengan sistem operasi Windows dapat berkomunikasi dengan komputer Sun-SPARC yang menjalankan Solaris. Jadi, jika sebuah komputer menggunakan protokol TCP/IP dan terhubung ke internet, maka komputer tersebut dapat berhubungan langsung dengan komputer lain dibelahan dunia manapun yang juga terhubung dengan internet.

TCP/IP berfungsi melakukan komunikasi data pada jaringan komputer. TCP/IP terdiri atas sekumpulan protocol yang masing-masing bertanggung jawab atas bagian-bagian tertentu dari komunikasi data. Jadi tugas masing-masing protokol menjadi jelas dan sederhana. Protokol yang satu tidak perlu mengetahui cara kerja protokol yang lain, sepanjang ia masih bisa saling mengirim dan menerima data.

3.2.2. Sejarah TCP/IP

Konsep TCP/IP berawal dari kebutuhan DoD (Departement of Defense) USA akan suatu komunikasi di antara berbagai variasi komputer yang telah ada. Komputer-komputer DoD ini seringkali harus menghubungkan antara satu organisasi peneliti dengan organisasi peneliti lainnya. Komputer tersebut harus tetap berhubungan karena terkait dengan pertahanan negara dan sumber informasi harus tetap berjalan meskipun terjadi bencana alam besar, seperti ledakan nuklir. Oleh karenanya pada tahun 1969 dimulailah penelitian terhadap serangkaian protokol TCP/IP. Adapun tujuan penelitian tersebut adalah sebagai berikut.

a. Terciptanya protokol-protokol umum, (DoD memerlukan suatu protokol yang dapat dipergunakan untuk semua jenis jaringan).
b. Meningkatkan efisiensi komunikasi data.
c. Dapat dipadukan dengan teknologi WAN (Wide Area Network) yang telah ada.
d. Mudah dikonfigurasi.

Protokol-protokol TCP/IP dikembangkan lebih lanjut pada awal 1980 dan menjadi protokol standar untuk ARPAnet pada tahun 1983. Protokol-protokol ini mengalami peningkatan popularitas di komunitas pemakai ketika TCP/IP dapat diimplementasikan dengan sangat baik pada versi 4.2 BSD (Berkeley Standard Distribution) UNIX. Versi ini digunakan secara luas pada institusi penelitian dan pendidikan serta digunakan sebagai dasar dari beberapa penerapan UNIX komersial, termasuk SunOS dari Sun dan Ultrix dari Digital.

3.3 UDP

3.3.1 Pengertian UDP

Dalam Buku I Putu Agus Eka Pratama tahun 2014 dijelaskan bahwa UDP (User Datagram Protocol) merupakan salah satu protokol utama di dalam jaringan komputer, khususnya pada Transport Layer, yang bersifat Connectionless dan Unreliable. Connectionless dapat diartikan bahwa UDP tidak memerlukan adanya persiapan (setup) koneksi terlebih dahulu untuk memulai proses dan layanan di dalamnya. Unreliable atau tidak andal, memiliki bahwa UDP tidak melakukan pengecekan untuk keandalan didalam jaringan layaknya seperti protokol TCP. Serta memiliki Header UDP yang didalanya memuat SPI (Source Process Identification) dan DPI (Destination Process Identification).

3.3.2 Karakteristik UDP

Karakteristik dari UDP antara lain, yaitu sebagai berikut :

a. Connectionless (tanpa koneksi): Pesan-pesan UDP akan dikirimkan tanpa harus dilakukan proses negosiasi koneksi antara dua host yang hendak berukar informasi.
b. Unreliable (tidak andal): Pesan-pesan UDP akan dikirimkan sebagai datagram tanpa adanya nomor urut atau pesan acknowledgment. Protokol lapisan aplikasi yang berjalan di atas UDP harus melakukan pemulihan terhadap pesan-pesan yang hilang selama transmisi. Umumnya, protokol lapisan aplikasi yang berjalan di atas UDP mengimplementasikan layanan keandalan mereka masing-masing, atau mengirim pesan secara periodik atau dengan menggunakan waktu yang telah didefinisikan.
c. UDP menyediakan mekanisme untuk mengirim pesan-pesan ke sebuah protokol lapisan aplikasi atau proses tertentu di dalam sebuah host dalam jaringan yang menggunakan TCP/IP. HeaderUDP berisi field Source Process Identification dan Destination Process Identification.
d. UDP menyediakan perhitungan cheksum berukuran 16 bit terhadap keseluruhan pesan UDP.

3.3.3 Kegunaan UDP

UDP sering digunakan dalam beberapa tugas berikut:

a. Protokol yang "ringan" (lightweight): Untuk menghemat sumber daya memori dan prosesor, beberapa protokol lapisan aplikasi membutuhkan penggunaan protokol yang ringan yang dapat melakukan fungsi-fungsi spesifik dengan saling bertukar pesan. Contoh dari protokol yang ringan adalah fungsi query nama dalam protokol lapisan aplikasi Domain Name System.
b. Protokol lapisan aplikasi yang mengimplementasikan layanan keandalan: Jika protokol lapisan aplikasi menyediakan layanan transfer data yang andal, maka kebutuhan terhadap keandalan yang ditawarkan oleh TCP pun menjadi tidak ada. Contoh dari protokol seperti ini adalah Trivial File Transfer Protocol (TFTP) dan Network File System (NFS)
c. Protokol yang tidak membutuhkan keandalan. Contoh protokol ini adalah protokol Routing Information Protocol (RIP).
d. Transmisi broadcast: Karena UDP merupakan protokol yang tidak perlu membuat koneksi terlebih dahulu dengan sebuah host tertentu, maka transmisi broadcast pun dimungkinkan. Sebuah protokol lapisan aplikasi dapat mengirimkan paket data ke beberapa tujuan dengan menggunakan alamat multicast atau broadcast. Hal ini kontras dengan protokol TCP yang hanya dapat mengirimkan transmisi one-to-one. Contoh: query nama dalam protokol NetBIOS Name Service.

3.4 IP Address

3.4.1 Struktur IP Address

Pada IP versi 4 Alamat IP terdiri dari bilangan biner sepanjang 32 bit yang dibagi atas 4 segmen. Tiap segmen terdiri atas 8 bit yang berarti memiliki nilai desimal dari 0 - 255. Luas area dari

alamat IP (range address) yang bisa digunakan adalah dari 00000000.00000000.00000000.00000000 sampai dengan 11111111.11111111.11111111.11111111. Jadi, ada sebanyak 232 kombinasi address yang bisa dipakai diseluruh dunia (walaupun pada kenyataannya ada sejumlah IP Address yang digunakan untuk keperluan khusus). Jadi, jaringan TCP/IP dengan 32 bit address ini mampu menampung sebanyak 232 atau lebih dari 4 milyar host. Untuk memudahkan pembacaan dan penulisan, IP Address biasanya direpresentasikan dalam bilangan desimal. Jadi, range address di atas dapat diubah menjadi address 0.0.0.0 sampai address 255.255.255.255. Nilai desimal dari IP Address inilah yang dikenal dalam pemakaian sehari-hari.
Format IP Address:

Binary	Decimal
00000000.00000000.00000000.00000000	= 0.0.0.0
s/d	
11111111.11111111.11111111.11111111	= 255.255.255.255

Alamat IP versi 4 umumnya diekspresikan dalam notasi desimal bertitik (*dotted-decimal notation*), yang dibagi ke dalam empat buah oktet berukuran 8-bit. Dalam beberapa buku referensi, format bentuknya adalah **w.x.y.z**. Karena setiap oktet berukuran 8-bit, maka nilainya berkisar antara **0** hingga **255** (meskipun begitu, terdapat beberapa pengecualian nilai).

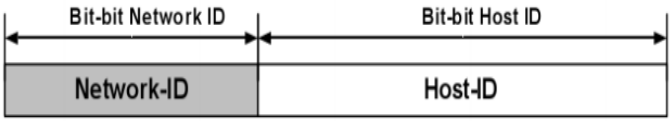
Alamat IP yang dimiliki oleh sebuah host dapat dibagi dengan menggunakan subnet mask jaringan ke dalam dua buah bagian, yakni:

a. *Network Identifier*/NetID atau *Network Address* (alamat jaringan) yang digunakan khusus untuk mengidentifikasikan alamat jaringan di mana host berada. Semua sistem di dalam sebuah jaringan fisik yang sama harus memiliki alamat

network identifier yang sama. *Network identifier* juga harus bersifat unik dalam sebuah *internetwork*. Alamat *network identifier* tidak boleh bernilai 0 atau 255.

b. *Host Identifier*/HostID atau *Host address* (alamat host) yang digunakan khusus untuk mengidentifikasikan alamat host di dalam jaringan. Nilai *host identifier* tidak boleh bernilai 0 atau 255 dan harus bersifat unik di dalam *network identifier* di mana ia berada.

IP Address dapat dipisahkan menjadi 2 bagian yaitu sebagai berikut :



3.4.2 Pembagian Kelas IP Address

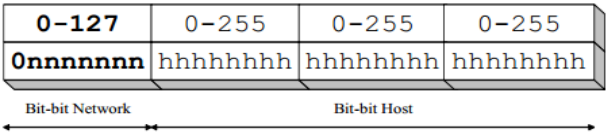
Jumlah IP address yang tersedia secara teoritis adalah 255x255x255x255 atau sekitar 4 milyar lebih yang harus dibagikan ke seluruh pengguna jaringan. Pembagian kelas-kelas ini ditujukan untuk mempermudah alokasi IP Address, baik untuk host/jaringan tertentu atau untuk keperluan tertentu.

Address dapat dipisahkan menjadi 2 bagian, yakni bagian network (net ID) dan bagian host (host ID). Net ID berperan dalam identifikasi suatu network dari network yang lain, sedangkan host ID berperan untuk identifikasi host dalam suatu network. Jadi, seluruh host yang tersambung dalam jaringan yang sama memiliki net ID yang sama. Sebagian dari bit-bit bagian awal dari IP Address merupakan network bit/network number, sedangkan sisanya untuk host. Garis pemisah antara bagian network dan host tidak tetap, bergantung kepada kelas network. IP address dibagi ke dalam lima kelas, yaitu kelas A, kelas B, kelas C, kelas D dan kelas E. Perbedaan tiap kelas adalah pada ukuran dan jumlahnya. Contohnya IP kelas A dipakai oleh sedikit jaringan namun jumlah host yang dapat

ditampung oleh tiap jaringan sangat besar. Kelas D dan E tidak digunakan secara umum, kelas D digunakan bagi jaringan multicast dan kelas E untuk keprluan eksperimental. Perangkat lunak Internet Protocol menentukan pembagian jenis kelas ini dengan menguji beberapa bit pertama dari IP Address.
Penentuan kelas ini dilakukan dengan cara berikut :

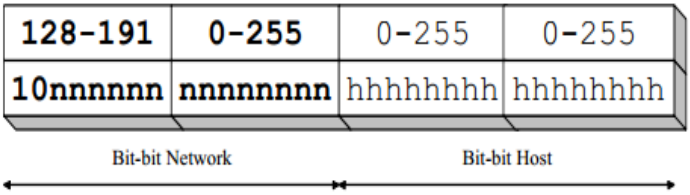
a. Kelas A

Bit pertama IP address kelas A adalah 0, dengan panjang net ID 8 bit dan panjang host ID 24 bit. Jadi byte pertama IP address kelas A mempunyai range 0-127. Jadi kelas A terdapat 127 network dengan tiap network dapat menampung sekitar 16 juta host (255 x 255 x 255). IP address kelas A diberikan untuk jaringan dengan jumlah host yang sangat besar, IP kelas ini dituliskan pada gambar berikut ini.



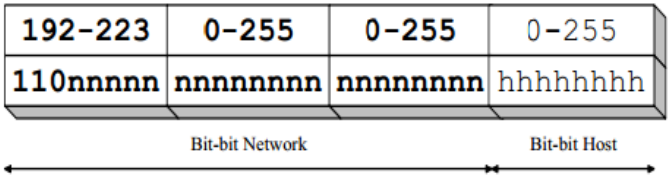
b. Kelas B

Dua bit IP address kelas B selalu diset 10 sehingga byte pertamanya selalu bernilai antara 128-191. Network ID adalah 16 bit pertama dan 16 bit sisanya adalah host ID sehingga kalau ada komputer mempunyai IP address 192.168.26.161, network ID = 192.168 dan host ID = 26.161. Pada. IP address kelas B ini mempunyai range IP dari 128.0.xxx.xxx sampai 191.155.xxx.xxx, yakni berjumlah 65.255 network dengan jumlah host tiap network 255 x 255 host atau sekitar 65 ribu host.



c. Kelas C

IP address kelas C mulanya digunakan untuk jaringan berukuran kecil seperti LAN. Tiga bit pertama IP address kelas C selalu diset 111. Network ID terdiri dari 24 bit dan host ID 8 bit sisanya sehingga dapat terbentuk sekitar 2 juta network dengan masing-masing network memiliki 256 host.



d. Kelas D

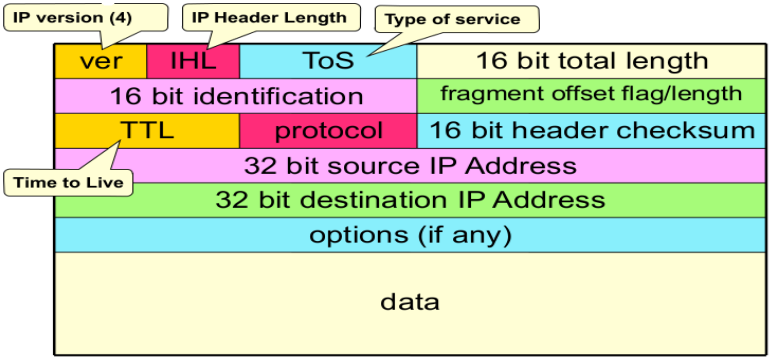
IP address kelas D digunakan untuk keperluan multicasting. 4 bit pertama IP address kelas D selalu diset pertamanya berkisar antara 224-247, sedangkan bit-bit berikutnya diatur sesuai keperluan multicast group 1110 sehingga byte yang menggunakan IP address ini. Dalam multicasting tidak dikenal istilah network ID dan host ID.

e. Kelas E

IP address kelas E tidak diperuntukkan untuk keperluan ekspiremental . 4 bit pertama IP address kelas ini diset 1111 sehingga byte pertamanya berkisar antara 248-255.

3.4.3 IP Header

IP header adalah informasi dimana IP protocol menambahkan di depan transport klien layer X untuk membuat IP paket. Header ini panjangnya 20 byte dan mencakup source dan destination IP address. Header-header IP diilustrasikan dalam datagram dibawah ini.



Fungsi dari masing-masing komponen diatas adalah sebagai berikut.

a. **Version (4 bit)**
   Header ini mendefinisikan versi Internet Protocol yang digunakan, versi yang secara luas banyak digunakan adalah versi 4.
b. **IHL (4 bit)**
   Header ini mendefinisikan panjang header IP dalam 32 bit word. Nilai minimum yang valid adalah 5 dan maksimumnya 6.
c. **Type of Service (8 bit)**
   Merupakan header yang menentukan bagaimanan proses transmisi datagram secara benar.
d. **Packet Length (16 bit)**
   Header yang mendefinisikan total panjang header dan data pada IP
e. **Identification (16 bit)**
   Header ini untuk mendukung fasilitas fragmentasi
f. **DF (1 bit)**

Header ini untuk mendifinisikan agar transmisi tidak di fragmentasi

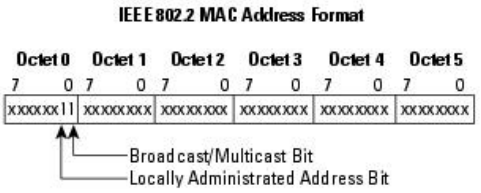
g. **DM (1 bit)**
   Header ini untuk mendifinisikan bahwa ada paket yang difragmentasi pada paket-paket berikutnya (More Fragment)
h. **Fragment Offset (13 bit)**
   Header ini mendefinisikan lokasi dari paket-paket yang mengalami fragmentasi dalam urutan keseluruhan paket
i. **TTL (16 bit)**
   Time to Live merupakan header yang mendefiniskan umur paket data, TTL akan berkurang 1 jika melewati sebuah router, demikian seterusnya sampai paket sampai ke host tujuan. Dengan mekanisma ini, dapat diantisipasi dimana paket bergentayangan terus di internet sehingga banyak terdapat paket sampah di internet jika ternyata host tujuan tidak ditemukan. Jika TTL telah habis (bernilai 0) sedangkan paket data
   belum sampai ke host tujuan, maka paket data akan dibuang.
j. **Transport (8 Bit)**
   Header ini mendefiniskan protokol pada layer transport yang digunakan, header ini bisa berupa TCP atau
   UDP
k. **Header Checksum (32 Bit)**
   Header ini digunakan untuk mengecek apakah terjadi perubahan/kerusakan pada header IP. Header Checksum dikalkulasi pada tiap router.
l. **Sending Address (32 Bit)**
   Sending Address atau Source Address merupakan header yang mendefinisikan IP address dari host asal.
m. **Destionation Address (32 Bit)**
   Destination Address merupakan header yang mendefinisikan IP address dari host tujuan.
n. **Option (32 Bit)**
   Header ini digunakan untuk mendefinisikan informasi tambahan pada layer transport seperti source
   routing.
o. **Padding (32 Bit)**

Header ini sama dengan padding pada TCP, yaitu digunakan untuk memenuhi panjang header sehingga merupakan kelipatan 32 bit. Jika terdapat header yang kurang, maka padding ditambahkan sampai berjumlah 32 bit

3.5 MAC Address

MAC Address (Media Access Control address) adalah alamat fisik suatu interface jaringan (seperti ethernet card pada komputer, interface/port pada router, dan node jaringan lain) yang bersifat unik dan berfungsi sebagai identitas perangkat tersebut . Secara umum MAC Address dibuat dan diberikan oleh pabrik pembuat NIC (Network Interface Card) dan disimpan secara permanen pada ROM (Read Only Memory) perangkat tersebut. MAC address juga biasa disebut Ethernet Hardware Address (EHA), Hardware Addres, atau Physical Address.

MAC Address memiliki panjang 48-bit (6 byte). Format standard MAC Address secara umum terdiri dari 6 kelompok digit yang masing-masing kelompok berjumlah 2 digit heksadesimal. masing-masing kelompok digit dipisahkan tanda (-) atau (:),



Supaya komputer dan perangkat jaringan lain bisa berkomunikasi satu dengan yang lain, frame-frame / data yang dikirim melalui jaringan harus memiliki MAC Address. Tetapi agar komunikasi jaringan lebih mudah dan sederhana, digunakanlah IP Address. Karena komunikasi jaringan menggunakan MAC Address maka alamat IP tersebut harus diterjemahkan ke MAC Address. Maka dari itu diciptakanlah ARP (Address Resolution Protocol)

yang bertugas untuk menerjemahkan IP Address menjadi MAC Address sehingga komputer pun bisa saling berkomunikasi.

3.6 Bahasa Pemrograman Python

Python merupakan bahasa pemrograman tingkat tinggi yang dapat berjalan di berbagai system operasi. Python adalah bahasa pemrograman interpretatif multiguna. Tidak seperti bahasa lain yang susah untuk dibaca dan dipahami, python lebih menekankan pada keterbacaan kode agar lebih mudah untuk memahami sintaks. Hal ini membuat Python sangat mudah dipelajari baik untuk pemula maupun untuk yang sudah menguasai bahasa pemrograman lain.

Pada laporan ini, Python dijalankan pada system operasi Ubuntu. Python pada Ubuntu tersedia secara default tanpa harus instalasi paket tambahan lagi. Untuk mengeceknya bisa dilakukan dengan mengetikkan “python” pada terminal Ubuntu.

Bahasa ini muncul pertama kali pada tahun 1991, dirancang oleh seorang bernama Guido van Rossum. Sampai saat ini Python masih dikembangkan oleh Python Software Foundation. Bahasa Python mendukung hampir semua sistem operasi, bahkan untuk sistem operasi Linux, hampir semua distronya sudah menyertakan Python di dalamnya.

Dengan kode yang simpel dan mudah diimplementasikan, seorang programmer dapat lebih mengutamakan pengembangan aplikasi yang dibuat, bukan malah sibuk mencari syntax error.

3.7 Ubuntu

Ubuntu merupakan varian atau turunan dari Debian, yang merupakan salah satu distro Linux tertua selain Red Hat & Slackware. Ubuntu diambil dari bahasa Afrika kuno yang berarti Humanity to Others atau rasa peri kemanusiaan terhadap sesama. Proyek Ubuntu dimulai pada tahun 2004 saat pengusaha bernama Mark Shuttleworth yang memilik perusahaan bernama Cannonical Ltd, mensponsori proyek Ubuntu. Keberadaan Ubuntu semakin kuat karena Canonical Ltd mempunyai support baik dari komunitas maupun professional.

Ubuntu dibentuk berdasarkan gagasan yang terdapat dalam filosofi Ubuntu, yaitu perangkat lunak harus tersedia secara gratis & tidak ada biaya lisensi, perangkat lunak harus dapat digunakan dalam bahasa lokal masing-masing & untuk orang-orang yang mempunyai keterbatasan fisik, serta bersifat open source sehingga pengguna memiliki kebebasan untuk mengubahnya sesuai dengan kebutuhan komputasi mereka. Kebebasan inilah yang membuat Ubuntu berbeda dari pesaingnya misalnya Microsoft Windows yang bersifat proprietary atau berlisensi. Saat ini Ubuntu dapat diperoleh secara gratis. Selain itu, kita mendapat kebebasan untuk memodifikasi Ubuntu agar menjadi distro Linux yang anda inginkan. Bahkan, anda dapat menamai sendiri versi Ubuntu hasil modifikasi tersebut.

3.7.1 Sejarah dan Perkembangan Ubuntu

Ubuntu pertama kali dirilis pada 20 Oktober 2004 dengan nomor versi 4.10. Semenjak itu, Canonical telah merilis versi Ubuntu yang baru 6 bulan sekali tiap bulan April dan Oktober. Setiap perilisan Ubuntu akan mempunyai nama kode dan nomor versi. Untuk codename Ubuntu terdiri dari dua kata yang berupa adjective (kata sifat) yang diikuti dengan nama hewan yang disusun secara alphabetis setiap rilisnya, kecuali versi 6.06 ke bawah. Sedangkan nomor versi berdasarkan tahun dan bulan dari rilis. Angka pertama adalah tahun, angka kedua adalah bulan perilisan. Setiap versi didukung selama 18 bulan untuk pembaruan sistem, keamanan, dan kesalahan (bug). Setiap 2 tahun sekali (versi xx.04 dengan x angka genap) akan mendapatkan Long Term Support (LTS) selama 3 tahun untuk desktop dan 5 tahun untuk edisi server. Namun mulai pada versi Ubuntu 12.04 yang dirilis pada April 2012 mendapatkan pembaruan sistem selama 5 tahun. Perpanjangan dukungan ini bertujuan untuk mengakomodasi bisnis dan pengguna IT yang bekerja pada siklus panjang dan pertimbangan biaya yang mahal untuk memperbarui sistem. Untuk saat ini, versi terakhir yang tersedia adalah Ubuntu 16.10 dengan code name “Yakkety Yak”

BAB IV
PELAKSANAAN PKL

4.1 Gambaran Umum Aplikasi

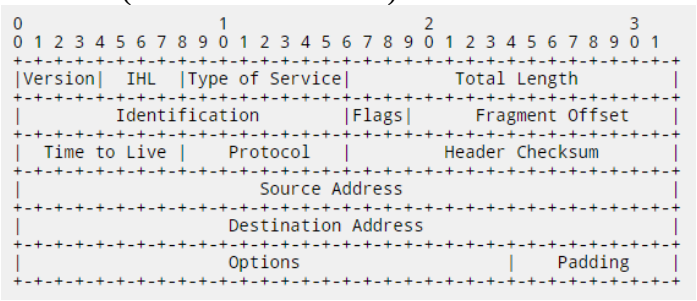
Dalam mengawasi traffic pada jaringan terdapat beberapa hal yang perlu diperhatikan seperti IP sumber dan tujuan paket jaringan, tipe paket jaringan (TCP/UDP), hingga port sumber dan port tujuan dari paket jaringan.

Aplikasi dikembangkan dengan bahasa pemrograman python. Bahasa pemrograman python dipilih karena python merupakan bahasa tingkat tinggi yang dapat berjalan diberbagai system operasi.

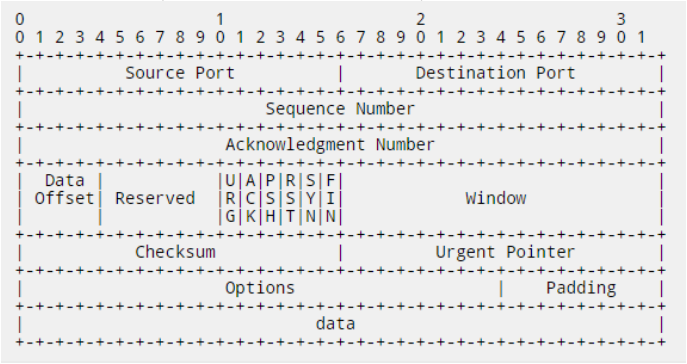
4.2 Skema Paket Jaringan

Sebelum membuat program paket sniffer kita perlu mengetahui bagian-bagian dari paket data jaringan yang ingin kita ambil. Berikut adalah skema dari beberapa tipe paket data jaringan berdasarkan protokol.

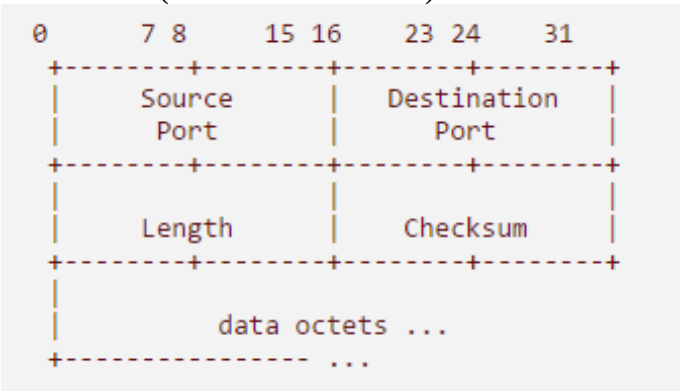
a. IP Header (berdasarkan RFC 791)



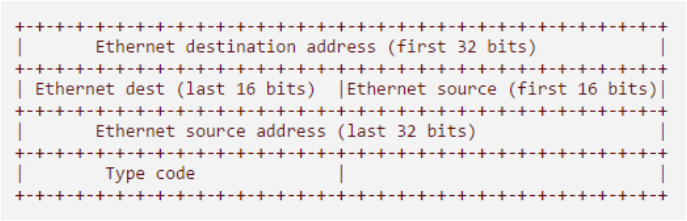
b. TCP Header (berdasarkan RFC 791)



c. UDP Header (berdasarkan RFC 768)



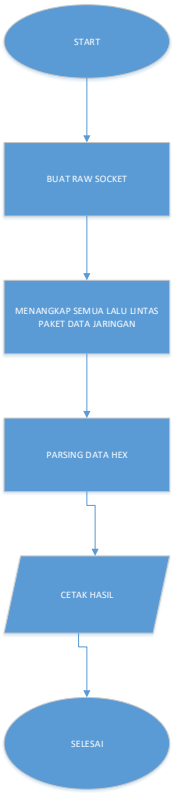
d. Ethernet Header



e. ICMP Header (berdasarkan RFC 792)

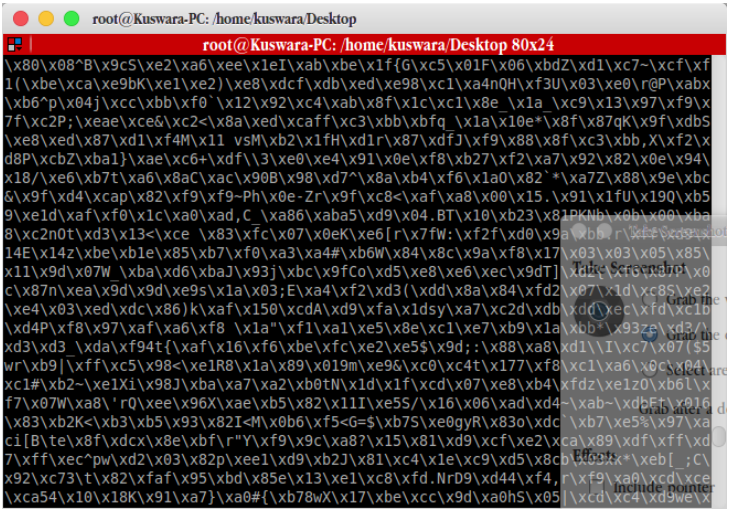
```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             unused                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Internet Header + 64 bits of Original Data Datagram      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

4.3 Flowchart Program



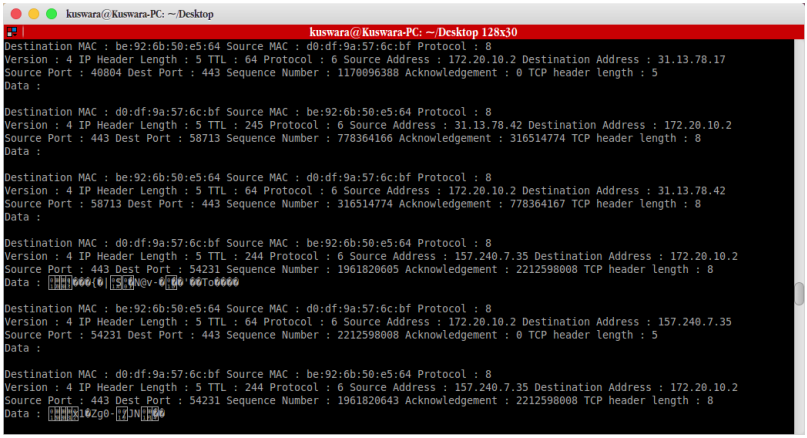
4.4 Implementasi dan Hasil

Program dibuat dengan bahasa Python dengan memanfaatkan library socket yang telah tersedia. Program dijalankan dengan akses root pada terminal Ubuntu. Awalnya program berhasil menangkap semua lalu lintas paket data jaringan seperti pada gambar xxx.xxx



Namun data tersebut hanya akan menampilkan data acak yang belum bisa dibaca karena data yang dihasilkan masih berupa data hex. Untuk mengatasi hal tersebut perlu dilakukan parsing dengan menggunakan fungsi unpack agar data tersebut bisa dibaca.

Fungsi unpack akan memecah packet jaringan menjadi IP Header, TCP Header, UDP header, ICMP header, dan data, sesuai dengan tipe paket data yang ditangkap.



Setelah data hex tersebut diparsing maka akan didapatkan data-data yang terdapat pada paket data jaringan berupa :

a. Destination MAC
b. Source Mac
c. Versi IP
d. Jenis Protokol
e. Source Address
f. Destination Address
g. Source port
h. Dentination port
i. Sequence number
j. Acknowledgement
k. Panjang header
l. Data

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil kegiatan yang telah dilakukan, dapat disimpulkan beberapa hal terkait dengan aplikasi packet sniffer, yaitu sebagai berikut :

a. Aplikasi packet sniffer dapat berjalan dengan baik pada system operasi Ubuntu dangan bahasa pemrograman Python.
b. Aplikasi packet sniffer mampu untuk menangkap beberapa tipe packet data seperti TCP, UDP, ICMP.

5.2 Saran

Adapun saran yang dapat disampaikan yaitu agar aplikasi yang dibuat dapat dikembangkan lebih lanjut sehingga dalam report yang dihasilkan menjadi lebih baik.