JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 03 NOMOR 01 JANUARI 2023
ISSN 2774 – 5775 | eISSN 2774-5767

IMPLEMENTASI METODE NETWORK ANALYZER PADA APLIKASI PENGELOLAAN DAN MONITORING JARINGAN PADA PT. SUMBER REZEKI

Agustinus Rio Trilaksono[1)], Luluk Harjanto[2)], Kevin Sendjaja[3)]
[1,2,3]Prodi Teknik Informatika, Fakultas Teknologi, ITB Swadharma

Correspondence author: A.R.Trilaksono, agustinusrio@yahoo.com, Jakarta, Indonesia

Abstract

Internet performance and security is very important, so that it can be used properly. All components on the network can be referred to as nodes, which send or receive data to exchange information. The data sent is divided into small parts in the form of network packets. At the company PT. Sumber Rezeki, the internet used has limited speed and quota, in daily activities it often goes down and the usage reports are still not detailed enough. A packet analyzer is needed in a network to be able to monitor a network so that the network remains safe and can run properly. Packet Analyzer can help monitor and detect attacks from hackers by monitoring oddities in network traffic. The purpose of this research is to design a packet analyzer program to perform network monitoring. The results of the design that was made went well according to plan based on the feasibility tests that had been carried out.

Keywords: computer network, network monitoring, packet analyzer

Abstrak

Performa dan keamanan internet sangat penting untuk diperhatikan, agar dapat digunakan dengan baik, lancar. Segala komponen yang berada di jaringan dapat disebut sebagai node, yang mengirimkan atau menerima data-data untuk bertukar informasi. Data-data yang dikirimkan dibagi menjadi bagian-bagian kecil dalam bentuk packet Network. Pada perusahaan PT. Sumber Rezeki, internet yang digunakan memiliki kecepatan dan kuota yang terbatas, dalam kegiatan sehari hari sering down dan laporan penggunaannya masih kurang terperinci. Diperlukan packet Analyzer dalam suatu jaringan untuk dapat mengawasi suatu jaringan agar jaringan tetap aman dan dapat berjalan dengan baik. Packet Analyzer dapat membantu mengawasi dan mendeteksi penyerangan dari hacker dengan mengawasi keanehan pada lalu lintas jaringan. Tujuan dari penelitian ini untuk merancang program packet Analyzer untuk melakukan Monitoring jaringan. Hasil rancangan yang dibuat berjalan dengan baik sesuai rencana berdasarkan uji kelayakan yang telah dijalankan.

Kata Kunci: jaringan komputer, monitoring jaringan, packet analyzer

A. PENDAHULUAN

Internet saat ini sudah merupakan hal yang sangat penting dalam kehidupan sehari-hari. Semua orang dapat berkomunikasi satu sama lain dari jarak yang sangat jauh dengan bantuan internet. Internet juga digunakan banyak orang dan perusahaan untuk membantu pekerjaannya (Subekti et al., 2021). Dengan adanya internet, banyak orang yang dapat terhubung satu dengan yang lain, berbagi informasi dan dapat melakukan pekerjaan bersama. Karena internet sangat penting, maka performa and keamanan internet sangat penting untuk diperhatikan, Sehingga internet dapat digunakan dengan baik dan lancar, serta dapat terjaga agar tetap aman.

Segala komponen yang berada di jaringan dapat disebut sebagai node (Komariah, 2016). Dalam penggunaan internet, nodes ini akan mengirimkan atau menerima data-data untuk dapat bertukar informasi. Data-data yang dikirimkan akan dibagi menjadi bagian-bagian yang lebih kecil dan dimuat dalam bentuk *packet network*. *Packet Network* memiliki format yang berbeda-beda sesuai dengan protokol yang digunakan (Nugroho et al., 2019). Selain berisi data yang akan dikirimkan, setiap packet Network juga memiliki informasi untuk membantu mengirimkan data dari sumbernya menuju tujuannya. Hal ini diperlukan karena terkadang *packet network* akan melewati banyak nodes untuk mencapai tujuannya, sehingga diberikan informasi tambahan agar data dapat terkirim ke tujuan yang tepat.

Proses pengiriman *packet network*, dapat ada masalah yang dapat mengganggu proses pengiriman packet network tersebut, gangguan koneksi dapat mengganggu proses pengiriman *packet network* (Dasmen & Rasmila, 2019). Hal ini menyebabkan data menjadi rusak. Gangguan pengiriman juga dapat menyebabkan delay pada waktu pengiriman, hal ini dapat membuat pekerjaan tertunda.

Network internet terbagi dalam beberapa topologi jaringan komputer (Fauzi et al., 2021; Santoso, 2016). Topologi jaringan komputer yang tidak lain adalah sebuah infrastruktur fisik dari sebuah jaringan komputer yang berfungsi untuk digunakan dalam mengimplementasikan LAN (Fitriansyah et al., 2019; Suhanda et al., 2022).

Adanya program yang tidak sedang dipakai namun tetap mengirim dan menerima data juga akan memperlambat koneksi internet. Dalam suatu jaringan juga dapat muncul serangan dari hackers, mereka dapat menyusupkan program untuk mencuri informasi. Hackers juga dapat menyerang suatu jaringan dengan banyak cara (Komariah, 2016). Hal-hal ini dapat mengganggu jaringan dan membuat jaringan tidak aman.

Packet Analyzer dapat digunakan untuk mengawasi suatu jaringan (Afdhal et al., 2015). Packet network akan melewati banyak nodes untuk mencapai tujuannya (Akmaluddin et al., 2019). Secara umum, node yang dilewati oleh packet network tersebut tidak akan memeriksa packet network jika node itu bukan tujuannya. Namun packet analyzer dapat membuat node tersebut menerima packet network yang dikirim walaupun node tersebut bukan tujuan packet network itu. Hal ini dapat membantu pengawas jaringan untuk mengawasi packet network, sehingga saat terjadi permasalahan dapat diatasi dengan cepat. Packet analyzer juga dapat membantu mendeteksi penyerangan dari hacker dengan mengawasi keanehan pada lalu lintas jaringan.

Pada PT. Sumber Rezeki, internet yang digunakan memiliki kecepatan dan kuota yang terbatas. Namun dalam kegiatan sehari hari, internet kantor sering down dan laporan penggunaan internet masih kurang terperinci. Hal ini menyebabkan pekerjaan para pekerja tertunda. Dari permasalahan tersebut, maka packet Analyzer diperlukan dalam suatu jaringan untuk dapat mengawasi suatu

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 03 NOMOR 01 JANUARI 2023
ISSN 2774 – 5775 | eISSN 2774-5767

jaringan agar jaringan tetap aman dan dapat berjalan dengan baik. Oleh karena itu alarm warning dengan packet Analyzer akan dirancang. Tujuan dari penelitian ini untuk merancang *packet analyzer* untuk melakukan monitoring jaringan.

B. METODE PENELITIAN

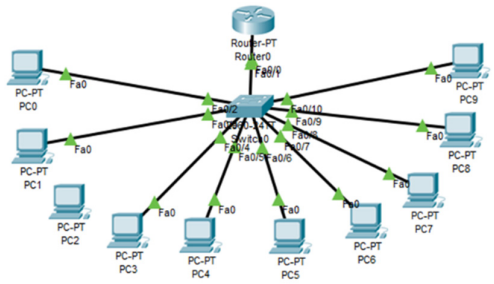
Metode penelitian yang digunakan adalah metode kualitatif dengan teknik pengumpulan data dengan teknik observasi dan wawancara (Sugiyono, 2017). Salah satu metode pengumpulan data dengan melakukan pengamatan informasi tentang proses yang ada, dokumen yang digunakan, dan laporan yang diperlukan, serta data lain yang diperlukan untuk perancangan dan pengembangan sistem aplikasi yang akan dikembangkan. Kegiatan wawancara dilakukan dengan manajer dan karyawan. PT. Sumber Rezeki sebuah perusahaan yang bergerak dalam bidang pemoles besi yang berlokasi di Tegal Alur Jakarta barat.

Metode yang digunakan Network Analyzers atau Ethernet Sniffer adalah sebuah aplikasi yang memiliki kemampuan melihat lalu lintas data pada jaringan komputer. Sebuah data akan mengalir secara bolak-balik pada jaringan, maka aplikasi ini menangkap tiap-tiap paket dan kadang-kadang menguraikan isi dari RFC (*Request for Comments*) atau spesifikasi yang lain.

Dari struktur jaringan yang ada seperti hub atau switch, dapat dipastikan salah satu pihak dapat menyadap keseluruhan atau salah satu dari pembagian lalu lintas dari salah satu mesin di jaringan. Perangkat pengendali jaringan dapat pula diatur oleh aplikasi penyadap untuk bekerja dalam mode *promiscuous mode* untuk "mendengarkan" semuanya yang pada umumnya pada jaringan kabel.

C. HASIL DAN PEMBAHASAN

Topologi jaringan yang ada sekarang pada PT. Sumber Rezeki yaitu sebagai berikut :



Gambar 1. Topologi Jaringan Yang Berjalan

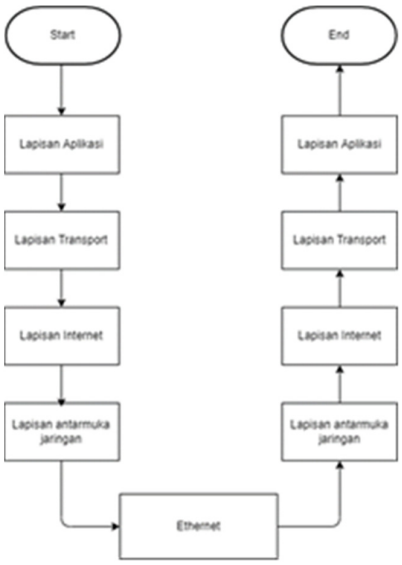
Berikut adalah tabel IP address PT. Sumber Rezeki:

Tabel 1. IP address

Nama	Alamat IP	Subnet Mask
Router0	192.168.1.1	255.255.255.0
PC0	192.168.1.2	255.255.255.0
PC1	192.168.1.3	255.255.255.0
PC2	192.168.1.4	255.255.255.0
PC3	192.168.1.5	255.255.255.0
PC4	192.168.1.6	255.255.255.0
PC5	192.168.1.7	255.255.255.0
PC6	192.168.1.8	255.255.255.0
PC7	192.168.1.9	255.255.255.0
PC8	192.168.1.10	255.255.255.0
PC9	192.168.1.11	255.255.255.0

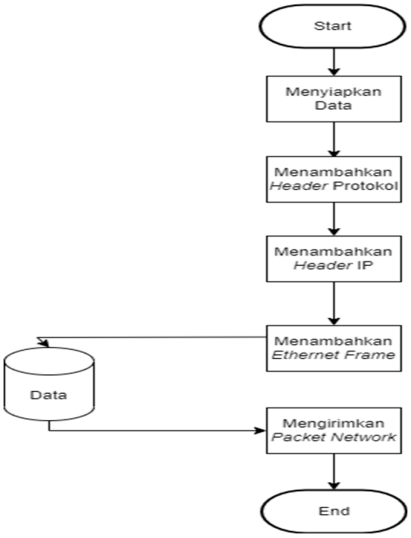
Pada sistem yang berjalan para karyawan menggunakan internet dalam pekerjaannya. Proses Monitoring dilakukan oleh manajer perusahaan, itu pun hanya hanya dapat mengecek total penggunaan internet dengan cara Login ke website ISP. Berikut adalah gambar Flowchart pengiriman data internet pada sistem berjalan:

D.



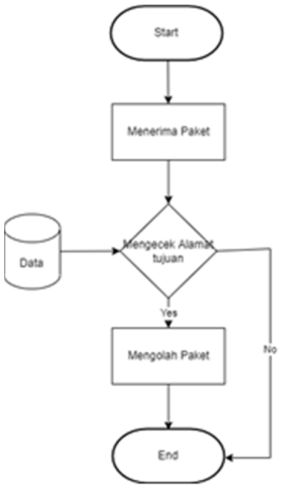
Gambar 2. Flowchart Internet pada sistem yang berjalan.

Berikut adalah gambar *flowchart* pengiriman data yang sedang berjalan ke komputer:



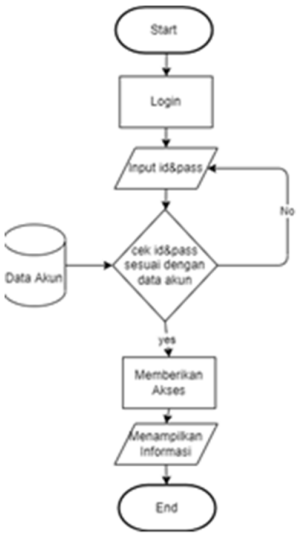
Gambar 3. Flowchart Pengiriman data yang sedang berjalan

Pada Flowchart gambar 3 dapat dilihat bahwa dalam pengiriman data internet, data akan melewati lapisan-lapisan TCP/IP. Flowchart diatas merupakan Flowchart pengiriman data, saat data akan dikirim, sistem akan mempersiapkan data dengan membagi mereka kedalam paket dengan ukuran kecil. Setelah itu paket akan ditambah Header protokol, Header ip, dan ethernet frame. Setelah itu baru data akan dikirim melalui ethernet. Berikut adalah gambar Flowchart penerimaan:



Gambar 4. *Flowchart* Penerimaan Data

Pada *flowchart* menerima, data yang dikirimkan ada di cek oleh PC, jika alamat tujuan yang ada di data sama dengan alamat PC, maka data akan diterima dan diproses. Jika tidak, maka data tidak diterima dan dibiarkan saja. Berikut adalah gambar Flowchart Monitoring:



Gambar 5. *Flowchart Monitoring*

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 03 NOMOR 01 JANUARI 2023
ISSN 2774 – 5775 | eISSN 2774-5767

Pada *Flowchart Monitoring*, Manajer akan *Login* ke website ISP, lalu setelah *Login* maka manajer dapat melihat informasi mengenai internetnya, hal ini meliputi kecepatan *bandwidth internet* dan kuota internet.

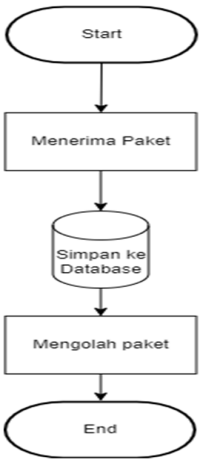
Analisis Kebutuhan Informasi

Proses Monitoring hanya dapat dilakukan dengan mengecek kuota pada ISP. Laporan ini tidak lengkap karena hanya memiliki informasi mengenai jumlah penggunaan total. Dibutuhkan beberapa laporan antara lain:

Laporan Network packet total, Laporan paket keluar dan masuk, Laporan IP belum terdaftar.

Rancangan Sistem Usulan

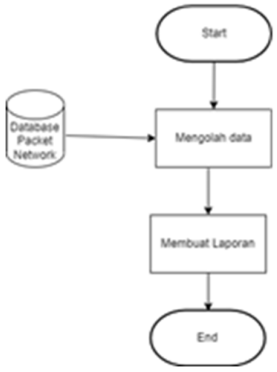
Pada *flowchart* yang berbeda dari sistem usulan ada pada proses penerimaan data.



Gambar 6. Flowchart menerima data usulan

Flowchart diatas merupakan Flowchart penerimaan data. Data yang akan diterima akan langsung dimasukan ke database. Setelah itu packet data baru akan diolah.

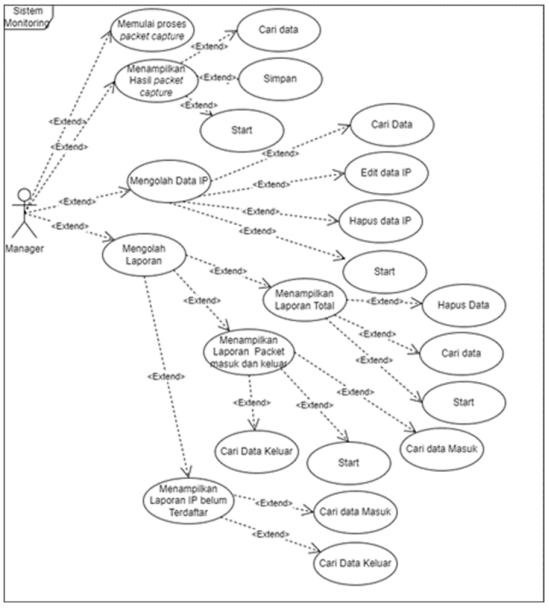
Berikut adalah Flowchart laporan:



Gambar 7. Flowchart laporan

Flowchart diatas merupakan Flowchart laporan. Dalam sistem usulan, pembuatan laporan dapat dilakukan dengan mengolah data yang telah dimasukan kedalam database. Proses monitoring pada aplikasi digambarkan dalam diagram Use case dibawah ini.

Use Case diagram proses Monitoring dan pengolahan laporan



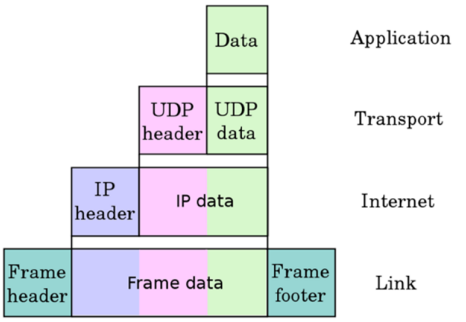
Gambar 8. Use Case Monitoring

Pada Use Case ini dapat dilihat proses yang dapat dilakukan oleh Manajer.

Cara kerja Packet Analyzer

Packet Analyzer merupakan program yang bertugas untuk menangkap semua paket

data yang melewati adapter. Berikut adalah gambar paket data yang terus mendapatkan Header pada setiap Layer:

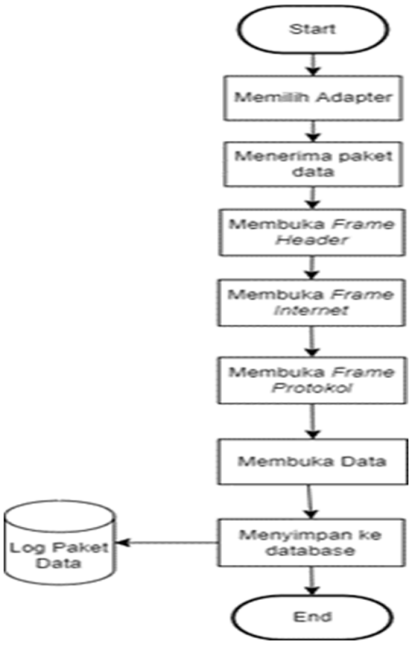


Gambar 9. Process Header

Dari gambar diatas dapat dilihat bahwa setiap melewati *layer* pada internet, maka data akan ditambah oleh *Header* sesuai dengan protokol yang digunakan.

Packet Analyzer juga dapat menggunakan *promiscuous mode* yaitu mode yang membuat *packet Analyzer* dapat menerima paket data yang bukan dikirimkan untuk adapternya.

Berikut adalah Flowchart proses kerja packet Analyzer:



Gambar 10. Flowchart proses kerja packet Analyzer

Langkah awal yang harus dilakukan dalam penggunaan packet Analyzer yaitu menentukan adapter yang akan dicatat datanya. Sebagai contoh paket data yang akan dibongkar yaitu paket data dengan protokol TCP dan IPv4

Setelah memilih Adapter, packet Analyzer akan mulai mengambil data. Data yang diambil akan diproses, Paket data yang telah diambil akan dibongkar untuk mengetahui informasi informasi yang ada didalamnya.

Dalam proses pembongkaran paket, paket akan dibongkar dari Layer per Layer. Setiap protokol akan memiliki format Header yang berbeda-beda. Setiap Header menampung informasi yang berbeda beda.

Header pertama yang akan dibongkar adalah ethernet Header. Dalam ethernet Header dapat diketahui data-data mengenai MAC Address pengirim dan tujuan, seperti destination address: E0-D5-5E-71-20-32, source address: F0-8C-FB-30-96-60. Dari ethernet Header ini juga dapat diketahui protokol apa yang digunakan seperti protokol: 0x0800. 0x0800 pada protokol ethernet Header menunjukan bahwa protokol yang digunakan adalah Ipv4. Ethernet Header memiliki size yang tetap yaitu 14 Bytes

Setelah membongkar *ethernet Header,* berikutnya yang akan dibongkar adalah *IP Header*. Dalam *IP Header* dapat didapatkan data data seperti:

1. versi IP
2. panjang *IP Header* dalam satuan Bytes.
3. Type Of Service berisi lima sub bidang yang menentukan jenis prioritas, penundaan, throughput, dan keandalan yang diinginkan untuk paket itu, namun *Type Of Service* sudah jarang digunakan dan biasanya diisi dengan 0.
4. Total panjang IP dapat ditemukan dalam *Header* ini dalam satuan Bytes.
5. Identifikasi yaitu adalah bidang identifikasi dan terutama digunakan untuk mengidentifikasi secara unik kelompok fragmen dari datagram IP tunggal.

6. Flags yaitu Bidang tiga bit mengikuti dan digunakan untuk mengontrol atau mengidentifikasi fragmen. Mereka adalah (secara berurutan, dari yang paling signifikan hingga yang paling tidak signifikan):
   a. bit 0: Dicadangkan; harus nol.
   b. bit 1: Jangan Pecah (DF)
   c. bit 2: Lebih Banyak Fragmen (MF)
   Jika Flag DF diset, dan fragmentasi diperlukan untuk merutekan paket, maka paket akan di-drop. Ini dapat digunakan saat mengirim paket ke host yang tidak memiliki resource untuk melakukan penyusunan fragmen.
7. TTL (*Time to Live*) yaitu Menentukan berapa lama datagram dapat tetap berada di Internet. Ini menjaga agar datagram yang salah rute tetap berada di Internet tanpa batas waktu.
8. Protokol, yaitu informasi mengenai protokol yang digunakan seperti 6 (TCP), 17(UDP), dll.
9. Checksum, yaitu Menunjukkan angka yang dihitung untuk memastikan integritas nilai Header
10. IP tujuan dan IP asal.

Setelah membongkar IP Header, maka yang akan dibongkar selanjutnya adalah protokol Header seperti TCP Header. Data yang dapat didapatkan setelah membongkar TCP Header yaitu:

1. Asal port dan tujuan port
2. Sequence Number, adalah penghitung yang digunakan untuk melacak setiap byte yang dikirim ke luar oleh sebuah host. Jika paket TCP berisi 1400 byte data, maka nomor urut akan bertambah 1400 setelah paket ditransmisikan.
3. ACK adalah Sequence Number berikutnya yang diharapkan oleh pengirim ACK. Ini mengakui penerimaan semua byte sebelumnya (jika ada). ACK pertama yang dikirim oleh masing-masing ujung mengakui nomor urut awal ujung lain itu sendiri, tetapi tidak ada data.
4. panjang Header dalam satuan Bytes
5. Flag, TCP Header memiliki beberapa Flags yaitu:
   a. SYN - digunakan sebagai langkah pertama dalam membangun koneksi antara dua host. Hanya paket pertama dari pengirim dan penerima yang harus memiliki Flag ini.
   b. ACK - Flag pengakuan digunakan untuk mengakui penerimaan paket yang berhasil. Seperti yang dapat kita lihat dari diagram di atas, penerima mengirimkan ACK serta SYN pada langkah kedua dari proses jabat tangan tiga arah untuk memberi tahu pengirim bahwa ia menerima paket awalnya.
   c. FIN - Flag selesai berarti tidak ada lagi data dari pengirim. Oleh karena itu, digunakan dalam paket terakhir yang dikirim dari pengirim.
   d. URG - Flag mendesak digunakan untuk memberitahu penerima untuk memproses paket-paket mendesak sebelum memproses semua paket lainnya. Penerima akan diberitahu ketika semua data penting yang diketahui telah diterima.
   e. PSH - Flag push agak mirip dengan Flag URG dan memberitahu penerima untuk memproses paket-paket ini saat diterima alih-alih menyangganya.
   f. RST - *Flag reset* dikirim dari penerima ke pengirim ketika sebuah paket dikirim ke host tertentu yang tidak mengharapkannya.
   g. ECE - *Flag* ini bertanggung jawab untuk menunjukkan apakah TCP mampu ECN.
   h. CWR - *Flag* yang dikurangi jendela kemacetan digunakan oleh host pengirim untuk menunjukkan bahwa ia menerima paket dengan *set Flag ECE.*
   i. NS (eksperimental) - Flag nonce sum masih merupakan Flag eksperimental yang digunakan untuk membantu

melindungi dari penyembunyian paket yang tidak disengaja dari pengirim.

6. *Window*, yaitu Ukuran *window* penerimaan, yang menentukan jumlah unit ukuran *window* yang ingin diterima oleh pengirim segmen ini.
7. *Checksum*, Memverifikasi integritas Header dan data segmen.
8. *Urgent pointer,* Menunjukkan data yang akan dikirimkan secepat mungkin. Pointer ini menentukan posisi dimana data urgent berakhir.

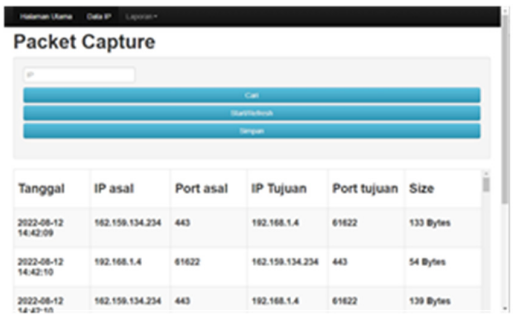
Setelah membongkar *TCP Header*, maka data paket data bisa dilihat dalam bentuk *Hexadecimal.* Sebagian besar protokol internet sudah melakukan enkripsi terhadap data paket yang dikirimkan sehingga data yang didapatkan akan sulit dibaca.

Dalam penyusunan program *packet Analyzer* ini. Program akan dibuat untuk membaca paket data secara terus menerus dalam *promiscuous mode*. Hasil dari paket paket data yang diterima akan disimpan dalam log file. Setelah proses penerimaan data berhenti, log file baru dapat diproses ke dalam database. Setelah log file dimasukan ke database, barulah data dapat dimanipulasi agar dapat menampilkan laporan sesuai dengan yang dibutuhkan.

Tampilan Struktur Menu Program

Halaman Utama

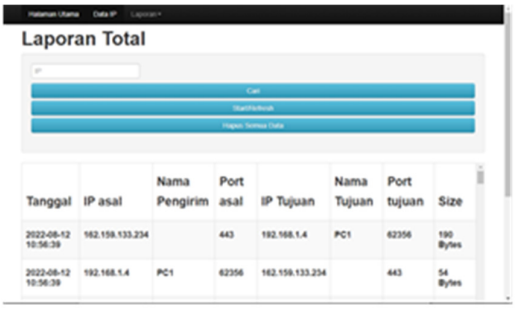
Halaman ini merupakan halaman utama sistem ini, dalam halaman ini terdapat menu untuk melihat hasil *packet capture*. Berikut adalah gambar tampilan halaman utama:



Gambar 11. Tampilan Halaman Utama

Halaman Laporan Total

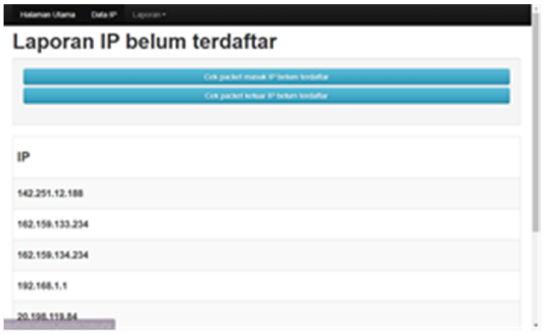
Halaman ini merupakan halaman utama sistem ini, dalam halaman ini terdapat menu untuk melihat Laporan total hasil *packet capture*. Berikut adalah gambar tampilan laporan total:



Gambar 12. Tampilan Laporan Total

Halaman Laporan belum terdaftar

Halaman ini merupakan halaman utama sistem ini, dalam halaman ini terdapat menu untuk melihat Laporan ip belum terdaftar. Berikut adalah gambar tampilan laporan *packet ip* belum terdaftar:

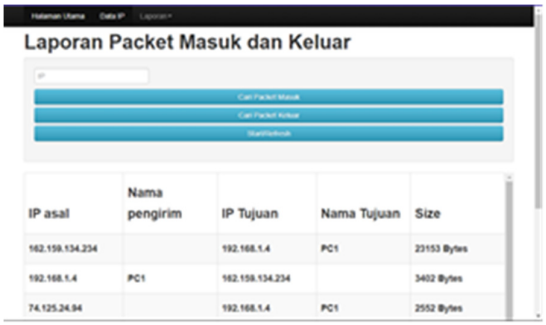


Gambar 13. tampilan laporan IP belum terdaftar

Halaman Laporan *packet* masuk dan keluar

Halaman ini merupakan halaman utama sistem ini, dalam halaman ini terdapat menu untuk melihat Laporan total hasil *packet capture*. Berikut adalah gambar tampilan laporan total:

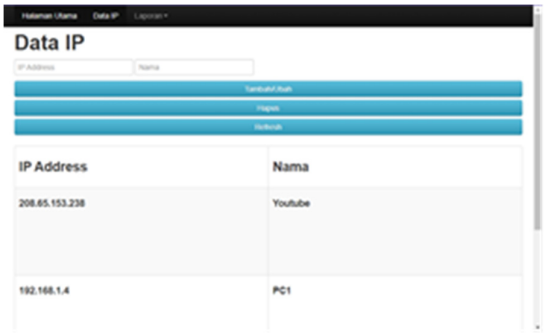
JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 03 NOMOR 01 JANUARI 2023
ISSN 2774 – 5775 | eISSN 2774-5767



Gambar 14. tampilan laporan paket keluar masuk

Halaman nama_ip

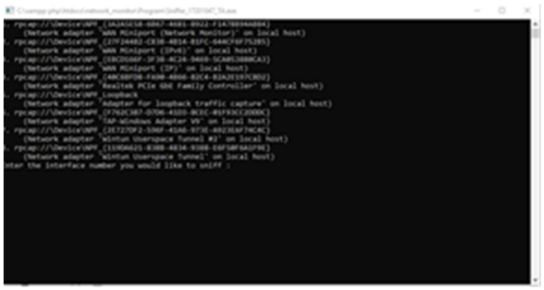
Halaman ini merupakan halaman utama sistem ini, dalam halaman ini terdapat menu untuk melihat dan menambahkan data ip. Berikut adalah gambar tampilan data user



Gambar 15. halaman data IP

Tampilan Program *Packet Capture*

Berikut adalah tampilan untuk program *packet capture*



Gambar 16. tampilan program *packet capture*

Hasil uji yang telah dilakukan sistem monitoring yang dirancang berjalan dengan baik, dapat memantau ip address, sehingga dapat mengetahui Ip address pada jaringan yang ada.

E. PENUTUP

Setelah melakukan penelitian terhadap sistem jaringan pada PT. Sumber Rezeki, maka dapat disimpulkan bahwa hasil pengujian sistem menunjukan dapat membantu menyediakan informasi mengenai lalu lintas paket data pada jaringan, proses pengolahan data monitoring menjadi lebih detail.

Sistem yang dirancang dapat membantu mengawasi jaringan di kantor dan membuat laporan lebih cepat dan lebih detail.

Untuk penelitian selanjutnya disarankan untuk menambahkan fitur real time dan menambah fitur-fitur analisis lainnya.

E. DAFTAR PUSTAKA

Afdhal, Munadi, R., & Fachdil, I. (2015). Evaluasi Kinerja VLAN Trunking Protocol dengan Metode Spanning Trees Protocol Menggunakan GNS-3. *Seminar Nasional Dan Expo Teknik Elektro*.

Akmaluddin, A., Arini, A., & Masruroh, S. U. (2019). Evalusi Kinerja Hot Standby Router Protocol (HSRP) dan Gateway Load Balancing Protocol (GLBP) untuk Layanan Video Streaming. *Cyber Security Dan Forensik Digital*, *2*(1), 43–51. https://doi.org/10.14421/csecurity.2019.2.1.1445

Dasmen, R. N., & Rasmila. (2019). Rancang Bangun VLAN Pada Jaringan Komputer RRI Palembang Dengan Simulasi Cisco Packet Tracer. *Jurnal Teknologi*, *Vol. 11 No*(1), 47–56.

Fauzi, S., Larasati, S., Putri, A. A., Restyasari, N., & Muhammad, G. (2021). Simulasi Multi-topologi Jaringan Berbasis SDN dengan Controller POX. *Journal*

TELNECT, *1*(2), 77–84.

Fitriansyah, A., Andreansyah, A., & Sopian, A. (2019). Penerapan Static VLAN Dan Access List Untuk Meningkatkan Keamanan Jaringan. *Jurnal Teknologi Informatika & Komputer*, *5*(2), 58–63.

Komariah, D. (2016). *Security Management Control Pada Jaringan Komputer*. Fakultas Ilmu Komputer Universitas Sriwijaya.

Nugroho, E. P., Nugraha, E., & Zulfikar, M. N. (2019). Sistem Reporting Keamanan pada Jaringan Cloud Computing Melalui bot Telegram dengan Menggunakan Teknik Intrussion Detection and Prevention System. *Jurnal Teknologi Terpadu*, *5*(2), 49–57. https://doi.org/10.54914/jtt.v5i2.233

Santoso, K. (2016). Konfigurasi dan Analisis Performansi Routing OSPF pada Jaringan LAN dengan Simulator Cisco Packet Tracer Versi 6.2. *Jurnal Kajian Teknik Elektro*, *1*(1), 67–78.

Subekti, Z. M., Mukiman, K., Fadil, A. F. A., & Asyrofi, M. (2021). Penerapan Limit Akses Browsing Internet Pada Saat Jam Kerja di PT XYZ. *Jurnal Teknologi Terpadu*, *7*(1), 31–38.

Sugiyono. (2017). *Metode Penelitian Bisnis: Pendekatan Kuantitatif, Kualitatif, Kombinasi dan R&D*. Bandung : Alfabeta.

Suhanda, Y., Nurlaela, L., Dharmalau, A., & Widjojo, B. S. (2022). Perancangan Infrastruktur Jaringan Berbasis Aplikasi Packet Tracer Dengan Metode Hot Standby Router Protocol. *Teknologi Terpadu*, *8*(1), 9–16.