BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan ilmu pengetahuan dan teknologi saat ini begitu cepat yang mengakibatkan kebutuhan manusia akan teknologi telekomunikasi begitu tinggi. Pada era saat ini kebutuhan akan teknologi merupakan suatu kebutuhan yang tidak bisa di lepaskan dalam kehidupan sehari-hari. Banyak kegiatan yang di lakukan melibatkan teknologi salah satunya jaringan komputer.Jaringan komputer merupakan jaringan telekomunikasi untuk melakukan transmisi data antara dua komputer atau lebih. Proses transmisi data sangat di perlukan pada saat ini sehingga tidak heran jika jaringan komputer dapat dijumpai di hampir semua instansi, sekolah, bandara dan berbagai tempat lainnya.

Dalam perkembangan jaringan komputer saat ini masih begitu banyak masalah yang dihadapi, masalah yang sering dihadapi adalah masalah pada keamanan jaringan tersebut, permasalahn seperti ini dapat menghambat proses kerja dari jaringan komputer sehingga kegiatan pada lokasi jaringan dapat terganggu.

Tidak terkecuali pada Kantor Camat Wara Utara yang merupakan salah satu instansi pemerintahan yang ada di kota Palopo. Kantor Camat Utara Wara Utara Kota Palopo juga telah menggunakan jaringan komputer, Para pegawai menggunakan akses internet untuk mengelola data, bertukar informasi, pencarian informasi dan lain sebagainya. Sehingga tidak menutup kemungkinan sewaktu-waktu dapat mengalami serangan atau pembobolan pada sistem jaringannya. Pada Kantor Camat Wara Utara Kota Palopo belum diterapkan sistem keamanan serta monitoring penggunaan jaringan, untuk itu perlu diadakan perbaikan dari segi monitoring baik monitoring paket data, *client* serta monitoring *router* terhadap serangan yang berpotensi menyerang sistem jaringan.

Sistem monitoring jaringan merupakan hal yang cukup penting dan tidak dapat di pisahkan pada pengimplementasian jaringan komputer, baik monitoring penggunaan *hotspot* didalam sebuah jaringan komputer maupun paket data yang berlalu lalang pada jaringan, sehingga perlunya memantau paket data yang digunakan *user* pada jaringan. Permasalahan yang juga terjadi terhadap sistem

jaringan terkadang sulit diatasi karena kurang detailnya informasi yang didapatkan sehingga untuk mengatasi hal tersebut perlu diterapkan sistem monitoring jaringan yang tepat sehingga permasalah pada sistem jaringan komputer dapat diminimalisir dan dapat diatasi dengan baik.

Berdasarkan uraian latar belakang tersebut, maka penulis terdorong untuk mengambil judul penelitian "Implementasi Sistem Monitoring Jaringan Menggunakan Wireshark dan Telegram Sebagai Sistem Notifikasi pada Kantor Camat Wara Utara". Dengan diangkatnya judul ini diharapkan dapat berguna bagi Kantor Camat Wara Utara.

1.2 Rumusan Masalah

Berdasarkan latar belakang permasalahan yang telah diuraikan diatas, maka rumusan masalah pada penelitian ini adalah bagaimana implementasi sistem monitoring jaringan menggunakan wireshark dan telegram sebagai sistem notifikasi pada Kantor Camat Wara Utara?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan dari penelitian ini adalah untuk implemenentasi sistem monitoring jaringan menggunakan wireshark dan telegram sebagai sistem notifikasi pada kantor camat wara utara.

1.4 Manfaat Penelitian

Adapun manfaat yang ingin dicapai dalam penelitian ini antara lain:

1. Bagi Penulis

   Manfaat yang di dapatkan penulis dari penelitian ini adalah:

a. Mempraktekan ilmu akademis yang telah peneliti pelajari.
b. Memahami konsep dari proses pengimplementasian sistem monitoring keamanan jaringan.

2. Bagi Dunia Akademik

Manfaat yang didapatkan bagi dunia akademik yaitu dapat dijadikan referensi buku atau jurnal bagi peneliti lain yang ingin mengembangkan penelitian terkait.

3. Bagi Instansi Terkait

   Manfaat yang didapatkan untuk instansi terkait adalah:

a. Memudahkan *administrator* jaringan dalam melakukan pengawasan paket jaringan terhadap jaringan yang dikelola nya.
b. Membantu *administrator* jaringan dalam monitoring *user hotspot* serta mencegah serangan terhadap *router*.

BAB II
TINJAUAN PUSTAKA

2.1 Kajian Teori

Kajian teori dalam proses penelitian merupakan salah satu tahapan yang penting untuk diperhatikan oleh para peneliti. Kajian teori ini akan menjadi dasar yang kuat dalam sebuah penelitina yang dilakukan. Para ahli memberikan banyak defenisi teori dalam penelitian. Teori yang berkaitan sebagai dasar dalam proses karya tulis ini adalah sebagai berikut:

1. Implementasi

Menurut Hamalik (2007:237), penulis buku yang berjudul Dasar-dasar Pengembangan Kurikulum, bahwa Implementasi merupakan suatu penerapan ide, konsep, kebijakan, atau inovasi dalam bentuk tindakan praktis sehingga memberikan dampak, baik perubahan pengetahuan, ketrampilan, maupun nilai dan sikap.

Dengan demikian implementasi merupakan kegiatan menerapkan gagasan maupan ide dalam bentuk tindakan sehingga memberikan perubahan yang baik bagi pelaksanaan kegiatan.Implementasi biasanya dilakukan setelah perencanaan maupun kegiatan observasi sudah dianggap baik sehingga implementasi suatu tindakan atau pelaksanaan dari sebuah rencana yang sudah disusun secara matang dan terperinci.

Implementasi bermuara pada aktivitas, aksi, tindakan atau adanya mekanisme suatu sistem, implemantasi bukan sekedar aktivitas, tapi suatu kegiatan yang terencana dan untuk mencapai tujuan kegiatan (Usman, 2002:70).

Jadi implementasi dapat diartikan sebagai suatu proses atau suatu aktivitas yang di gunakan untuk mentransfer ide yang dituangkan dalam bentuk pengaktualisasian hasil observasi dan pengumpulan data.

Pengertian-pengertian di atas memperlihatkan bahwa kata implementasi bermakna pada aktivitas, penerapan, atau pelaksanaan suatu sistem. Ungkapan penerapan mengandung arti bahwa implementasi bukan sekadar aktivitas, tetapi suatu kegiatan yang terencana dan dilakukan secara sungguh-sungguh berdasarkan penelitian atau norma tertentu untuk mencapai tujuan kegiatan.

2. Pengertian Sistem

Sistem adalah elemen-elemen atau prosedur-prosedur yang disususn serta terintegrasi dengan tujuan bersama untuk mencapai sasaran tertentu (Rahmawati dan Bachtiar, 2018:78).

Dengan demikian sistem merupakan suatu keterkaitan antara elemen satu dan elemen lainnya yang bertujuan untuk mencapai suatu tujuan yang sama.

Wardhani (2017:10), menyatakan bahwa sistem merupakan suatu kesatuan terdiri dari dua atau lebih komponen atau sub sistem yang berinteraksi untuk mencapai suatu tujuan.

Sistem ialah suatu kumpulan/group dari sub sistem/bagian/komponen ataupun baik fisik maupun non fisik yang saling berhubungan satu sama lain dan bekerja sama dengan secara harmonis untuk mencapai satu tujuan tertentu (Susanto 2013:22).

Dapat disimpulkan bahwa sistem merupakan suatu kumpulan dari komponen-komponen yang saling bekerja dan saling berhubungan dalam mencapai tujuan tertentu.

3. Keamanan Jaringan

Keamanan jaringan adalah suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan (Sutarti dan Khairunisa 2017:8).

Keamanan jaringan didefinisikan sebagai perlindungan sumber daya terhadap pengungkapan yang tidak sah, modifikasi, pemanfaatan, larangan dan penghancuran oleh orang yang tidak dikenal (Wajong, 2012).

Menurut Diansyah (2015:12), keamanan jaringan secara umum merupakan komputer yang terhubung ke *network*, memiliki ancaman kemanan lebih besar dari pada komputer yang berdiri sendiri (*standalone*). Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi. Tetapi *network security* umumnya bertentangan dengan *network access* semakin praktis, maka *network security* semakin rawan serta bila *network security* semakin baik, *network access* semakin tidak nyaman. Suatu *network* didesain sebagai komunikasi data *highway* dengan tujuan menaikkan akses kesistem komputer, sementara *security* rancang untuk

mengontrol akses. Penyediaan *network security* merupakan aksi penyeimbang atara *open access* dengan *security*.

Jadi dapat disimpulkan bahwa keamanan jaringan adalah suatu cara atau metode untuk melindungi jaringan dari berbagai macam serangan yang akan merusak jaringan.

4. Jaringan Komputer

Jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputer, dalam bahasa populer dapat di jelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer, dan perangkat lain seperti *router*, *switch* dan sebagainya (Sofana, 2013:3).

Menurut Haryanto dan Riadi (2015), jaringan komputer adalah sebuah jaringan umumnya terdiri dari dua atau lebih komputer yang saling berhubungan diantara satu dengan yang lainnya, serta saling berbagi sumber daya misalnya *CDROM*, *Printer*, Pertukaran *file*, atau memungkinkan untuk saling berkomunikasi secara elektronik. Komputer yang terhubung dimungkinkan berhubungan dengan menggunakan media kabel, saluran telepon, gelombang radio, satelit atau *infrared*.

Jaringan komputer dapat diklasifikasikan menjadi beberapa jenis, mulai dari berdasarkan area atau letak geografis, fungsi, topologi, media transmisi, sumber data, dan berdasarkan proses data (Amien dan Mukhtar, 2020:8).

Sehingga dapat disimpulkan bahwa jaringan komputer merupakan sekumpulan komputer yang saling terkoneksi dan berhubungan satu sama lain sehingga dapat saling berbagi data dan informasi. Jaringan komputer dapat diklasifikasikan menjadi 4, yaitu:

a. LAN (*Local Area Network*)

Menurut Sopandi (2010:2), *Local Area Network* (LAN) adalah jaringan yang bersifat *internal* dan umumnya milik pribadi didalam sebuah perusahaan kecil atau menengah serta umumnya berukuran beberapa kilometer. LAN seringkali dipergunakan untuk menghubungkan komputer-komputer pribadi serta *workstation* pada kantor suatu perusahaan atau pabrik-pabrik untuk pemakaian

sumber daya beserta *resource* (*hardware* dan *software*) serta untuk saling bertukar informasi.

Jaringan LAN (*Local Area Network*) dibentuk dari sekumpulan komputer dan/atau perangkat lainnya yang saling terhubung, dan semuanya perangkat berada pada satu lokasi yang sama yang tidak begitu luas (Amien dan Mukhtar, 2020:8).

Jadi LAN (*Local Area Network*) merupakan jaringan yang mencakup daerah kecil dan terbatas, digunakan untuk menghubungkan komputer-komputer pada suatu kantor ataupun sekolah.

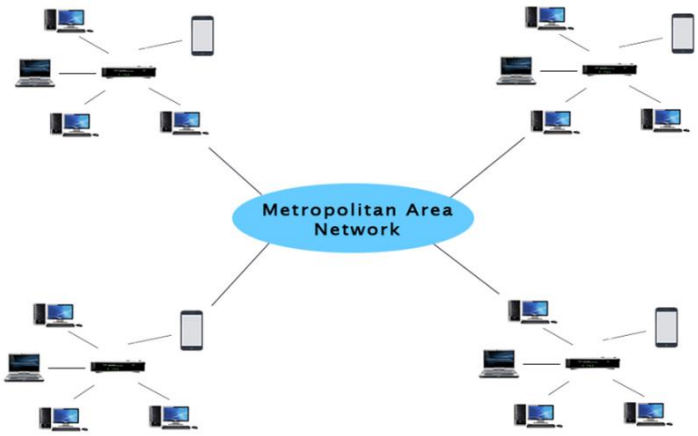
Gambar 1. LAN (*Local Area Network*)
Sumber: www.javatpoint.com

b. MAN (*Metropolitan Area Network*)

MAN merupakan jaringan yang meliputi area lebih besar dari LAN, misal antar wilayah pada satu provinsi. Pada hal ini jaringan MAN menghubungkan beberapa jaringan-jaringan kecil kedalam lingkungan area yang lebih besar, sebagai contoh jaringan pada kantor cabang sebuah bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya (Suranto, Prayogi dan Efendi, 2015:11).

Menurut Amien dan Mukhtar (2020:9), Jaringan MAN (*Metropolotan Area Network*) dibangun dengan menghubungkan jaringan-jaringan LAN, sehingga komunikasi pada jaringan MAN dapat mencakup area kota. Tujuan dari jaringan MAN untuk menghubungkan jaringan komputer yang berada pada suatu kota menjadi sebuah jaringan yang lebih besar.

Jaringan *Local Area Network* (LAN) merupakan jaringan yang cakupannya lebih luas dari Jaringan *Local Area Network*, sehingga jaringan MAN merupakan jaringan komputer yang menghubungkan jaringan-jaringan LAN.



Gambar 2.MAN (*Metropolitan Area Network*)
Sumber: www.javatpoint.com

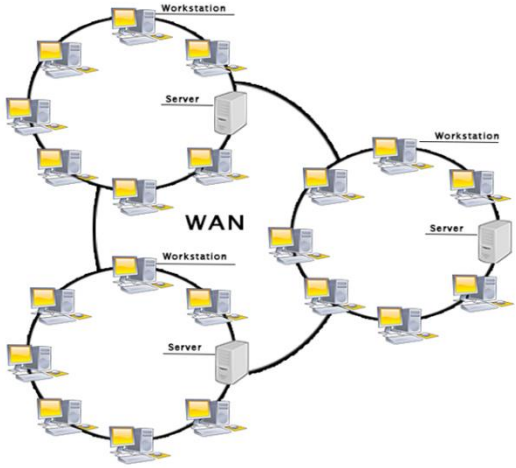
c. WAN (*Wide Area Network*)

Menurut Stallings (2007:49), WAN melingkupi wilayah yang luas, serta memerlukan pelitasan hak jalan publik, serta dapat bergantung sebagian kepada sirkuit yang di sediakan oleh penyedia jasa umum. Umumnya WAN terdiri dari beberapa simpul penyambungan (*switching node*) yang saling berhubungan. Suatu transmisi dari salah satu perangkat dirutekan melalui simpul-simpul *internal* ke perangkat tujuan yang telah di tentukan.

Wide Area Network (WAN) merupakan jaringan yang ruang lingkupnya telah menggunakan sarana satelit, *wireless* atau pun kabel *fiber* optik karena jangkauannya lebih luas, bahkan jangkauannya hingga wilayah dan negara lain (Ginta, Kusuma dan Negara, 2013:124).

Jaringan WAN merupakan jaringan yang mempunyai lingkup area yang sangat luas. Jaringan WAN dapat menghubungkan antar kota, bahkan negara dan benua. Media yang digunakan jaringan WAN menggunakan saluran komunikasi public (Amien dan Mukhtar, 2020:12).

Sehingga dapat disimpulkan bahwa jaringan *Wide Area Network* (WAN) merupakan kumpulan dari jaringan-jaringan yang berbeda yang saling terkoneksi denga cakupan wilayah yang luas.



Gambar 3. WAN (*Wide Area Network*)
Sumber: www.javatpoint.com

d. Internet

Kurniawan (2007:20), menegaskan bahwa internet merupakan gabungan dari berbagai LAN dan WAN yang berada diseluruh jaringan komputer di dunia, sehingga terbentuk jaringan dengan skala lebih luas dan global. Jaringan internet biasanya menggunakan protokol TCP/IP dalam hal mengirimkan paket data.Internet berasal dari kata *Interconnected Network* yang berarti hubungan dari berbagai jaringan komputer di dunia yang saling terkoneksidan membentuk suatu komunikasi global.

Internet (*interconnection networking*) sendiri adalah jaringan komunikasi global yang terbuka dan menghubungkan jutaan bahkan miliaran jaringan komputer dengan berbagai tipe dan jenis, dengan menggunakan tipe komunikasi seperti telepon, satelit dan sebagainya (Simpony dan Warnilah, 2020:1).

5. Topologi Jaringan

Menurut Halawa (2016:68), topologi jaringan komputer merupakan suatu cara untuk menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk sebuah jaringan. Dalam suatu jaringan komputer jenis topologi yang digunakan akan mempengaruhi kecepatan komunikasi, sehingga perlu dicermati kelebihan/keuntungan dan kekurangan/kerugian dari masing-masing topologi berdasarkan karakteristiknya.

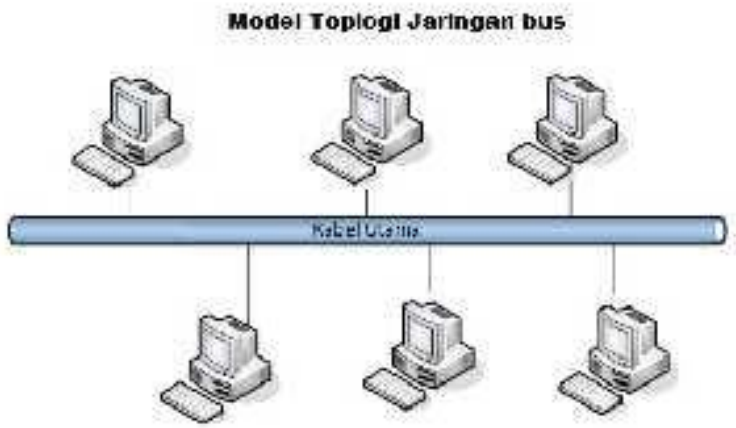
Madcoms (2015:8), menyatakan bahwa topologi jaringan ialah gambaran pola hubungan antara komponen jaringan, yang meliputi

komputer *server*, komputer *client*/*workstation*, *hub*/*switch*, pengkabelan serta komponen jaringan yang lain.

Topologi jaringan merupakan salah satu hal yang perlu di pertimbangkan saat membangun sebuah jaringan komputer, pemilihan sebuah topologi jaringan yang akan digunakan didasarkan pada skala jaringan yang akan dibuat. Topologi jaringan dapat diklasifikasikan menjadi 5, yaitu:

a. Topologi *Bus*

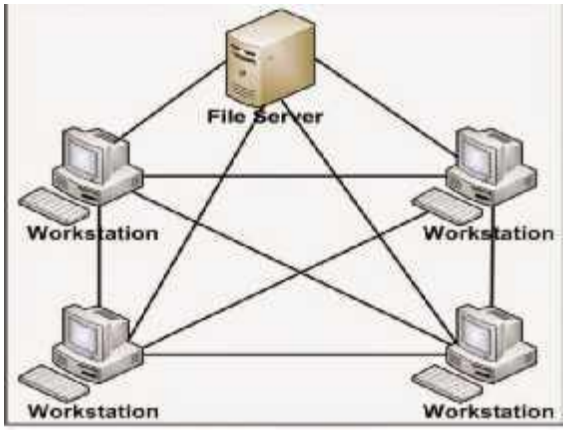
Menurut Herlambang (2008:10), topologi *bus* merupakan sebuah topologi yang menghubungkan semua terminal ke satu jalur komunikasi yang kedua ujungnya ditutup dengan *terminator*. *Terminator* merupakan perangkat yang menyediakan resistansi listrik untuk menyerap sinyal pada akhir transmisi sambungan sehingga sinyal tidak terlontar kembali dan diterima lagi oleh stasiun jaringan.



Gambar 4. Topologi *Bus*
Sumber: Sofana (2015:10)

b. Topologi *Mesh*

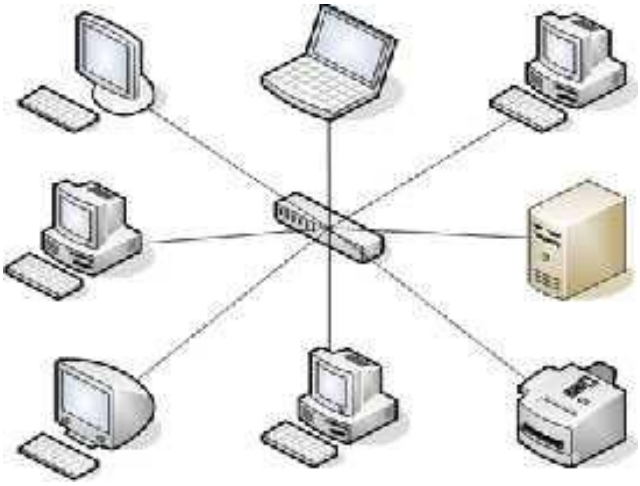
Zain (2016:14), menegaskan bahwa topologi jaringan *mesh* menghubungkan antar perangkat dimana setiap perangkat terhubung secara langsung ke perangkat lainnya yang berada di dalam jaringan. Pada topologi *mesh* setiap perangkat dapat berkomunikasi secara langsung dengan perangkat yang dituju (*Dedicated links*).



Gambar 5. Topologi *Mesh*
Sumber: Nugroho (2016:12)

c. Topologi *Star*

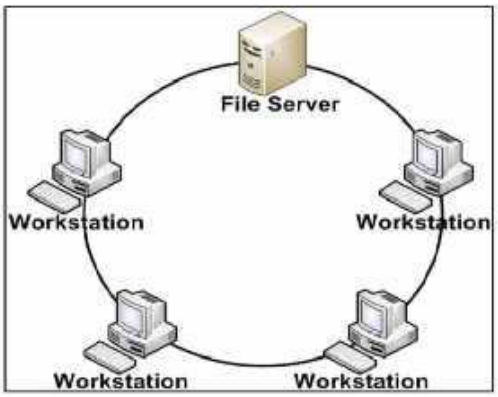
Wahyudi (2019), berpendapat bahwa dalam topologi *star*, sebuah terminal pusat bertindak sebagai pengatur serta pengendali semua komunikasi data. Terminal-terminal lain terhubung dan pengiriman data pada satu terminal ke terminal lainnya melalui terminal pusat. Terminal pusat menyediakan jalur komunikasi khusus untuk dua terminal yang akan berkomunikasi. Semua kontrol dipusatkan pada satu komputer stasiun primer dan komputer stasiun sekunder. Setelah hubungan jaringan dimulai, setiap stasiun sekunder dapat sewaktu-waktu menggunakan hubungan jaringan tanpa menunggu perintah dari stasiun primer.



Gambar 6. Topologi *Star*
Sumber: Nugroho (2016:11)

d. Topologi *Ring*

Topologi *ring* sangat berbeda dengan topologi bus. Jaringan yang menggunakan topologi *ring* dapat dikenali dari kabel *backbone* yang membentuk cincin.Setiap komputer yang terkoneksi dengan kabel *backbone*. Setelah sampai pada komputer terakhir maka ujung kabel akan kembali dihubungkan dengan komputer pertama (Sofana, 2015:22).

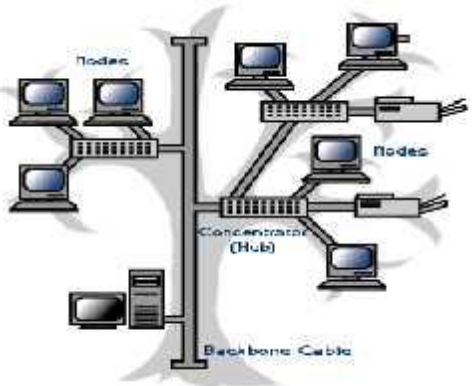


Gambar 7. Topologi *Ring*
Sumber: Sofana (2013:22)

e. Topologi *Tree*

Topologi *tree* merupakan perpaduan antara topologi *bus* dan *star*, yang terdiri dari kelompok-kelompok dari *Workstation* yang terkoneksi ke kabel utama menggunakan topologi *bus* (Daryanto, 2010:34).

Topologi ini memungkinkan untuk pengembangan jaringan yang telah ada dan memungkinkan sebuah perusahaan mengkonfigurasi jaringan sesuai dengan kebutuhannya.



Gambar 8. Topologi *Tree*
Sumber: Sofana (2015:54)

6. Protocol Jaringan

Protokol diartikan sebagai sebuah aturan atau standar yang mengatur dan mengijinkan terjadinya hubungan komunikasi dan perpindahan data dari satu ke dua atau lebih komputer (Pratama dan Dharmesta, 2019:96).

Ada beberapa jenis protokol yang digunakan pada jaringan dan internet, antara lain adalah TCP/IP, UDP, HTTP dan DNS.

a. *Transmission Control/Internet Protocol* (TCP/IP)

Menurut Santoso dan Gatot (2006), TCP/IP ialah jaringan terbuka yang bersifat independen terhadap prosedur transport pada jaringan fisik yang digunakan, sehingga bisa digunakan di mana saja. Protokol ini menggunakan skema pengalamatan yang sederhana yang disebut sebagai alamat IP (*IP Address*) yang mengizinkan banyak komputer untuk bisa saling terkoneksi satu sama lainnya di internet.

Menurut Tanembaum (2003), pada penggunaan internet serta secara *general* jaringan TCP/IP, pengomunikasian setiap *software* denganmenggunakan protokol pendukung. Protokol ini bagian di dalam layer transport (*transport layer*) pada standar OSI yaitu bagian yang memberkan efisiensi serta jaminan komunikasi *end-to-end*.

b. *User Datagram Protocol* (UDP)

Protokol UDP merupakan protokol yang bersifat *connectionless* dalam melakukan proses transmisi data.

Protokol UDP pada dasarnya hanya mengandung IP dengan tambahan *header* singkat. Protokol UDP tidak melakukan sebuah proses control jalur data, kontrol kesalahan ataupun pengiriman ulang terhadap kesalahan sehingga hanya menyediakan *interface* ke protokol IP (Mardiana dan Sahputra, 2017:76).

c. *Hypertext Transfer Protocol* (HTTP)

HTTP merupakan sebuah protokol yang meminta atau menjawab antara *client* dan *server*. Sebuh *client* HTTP seperti *web browser*, biasanya memulai permintaan dengan membuat hubungan TCP/IP ke *port* tertentu di tuan rumah yang jauh biasanya *port* 80 (Zabar dan Novianto, 2015:70).

Pengembangan HTTP dikoordinasi oleh *Konsorsium World Wide Web* (W3C) dan grup bekerja *Internet Engineering TaskForce* (IETF), bekerja dalam

publikasi satu seri RFC, yang paling terkenal RFC 2616, yang menjelaskan HTTP/1.1, versi HTTP yang digunakan umum sekarang ini

7. Perangkat Jaringan

a. *Switch*

Menurut Ginta (2013), *Switch* merupakan sebuah alat jaringan yang melakukan *bridging* transparan (penghubung segmentasi banyak jaringan dengan *forwarding* berdasarkan alamat MAC). *Switch* jaringan bisa digunakan sebagai penghubung komputer atau *router* di satu area yang terbatas, *switch* bekerja pada lapisan data *link*, cara kerja *switch* hampir sama seperti *bridge*, tetapi *switch* mempunyai sejumlah *port* sehingga sering dinamakan multi ± *port bridge*. *Switch* disebut sebagai multi port sebab mempunyai *collistindomain* dan *broadcastdomain* tersendiri, mampu mengatur lalu lintas paket yang melalui *switch* jaringan.

Gambar 9.*Switch*
Sumber : Sudirman (2013:145)

b. *Access Point*

Zain (2016), berpendapat bahwa *access point*merupakan sebuah perangkat jaringan yang berisi sebuah *transciever* dan atena untuk mentransmisikan dan menerima sinyal ke *client remote* dan dari *client remote*. Dengan *access point* (AP) *client wireless* dapat dengan cepat dan mudah untuk terhubung ke jaringan LAN secara *wireless. access point* yang ditempatkan diluar ruangan dilengkapi dengan *box outdoor* yang berfungsi sebagai pelindung dari cuaca seperti hujan maupun panas matahari, serta atena yang digunakan berbeda dengan atena yang digunakan didalam ruangan.

Gambar 10.*Access Point*
Sumber: www.cisco.com

c. *Bridge*

Menurut Kurniawan (2012), *bridge* adalah peralatan yang mampu menghubungkan beberapa segmen pada jaringan. Berbeda dengan *hub, bridge* mampu mempelajari *MAC address* tujuan. Sehingga ketika sebuah komputer mengirim data untuk komputer tertentu, bridge akan mengirim data melalui port yang terhubung dengan komputer tujuan saja. Ketika *bridge* belum mengetahui port mana yang terhubung dengan komputer tujuan, maka dia akan mencoba mengirim pesan *broadcast* ke semua *port* kecuali *port* komputer pengirim.

Gambar 11.*Bridge*
Sumber: Nursiyanta (2011:7)

d. *Router*

Menurut Sutomo (2010:3), *router* adalah sebuah perangkat yang digunakan dalam jaringan komputer yang dapat mengirimkan data ke jaringan lainnya melalui jalur yang lebih cepat, tepat dan efisien. *Router* berfungsi untuk meneruskan paket-paket dari *network* ke *network* yang lainnya (baik LAN ke LAN atau LAN ke WAN) sehingga *host-host* yang ada pada sebuah *network* dapat berkomunikasi dengan *host-host* yang ada pada *network* lainnya. *Router* menghubungkan *network-network* tersebut pada *network layer* dari model OSI, sehingga secara teknis *router* adalah *Layer 3 Gateway*.

Gambar 12. *Router*
Sumber: unnes.ac.id

e. Hub

Hub adalah peralatan yang dapat menggadakan *frame* data yang berasal dari satu komputer ke semua *port* yang ada pada *hub* tersebut. Sehingga semua *port* yang terhubung dengan port hub akan menerima data juga. *Hub* juga di gunakan pada jaringan *star* (Sofana, 2013:68).

Gambar 13. *Hub*
Sumber: www.dosenit.com

7. Jenis-Jenis Ancaman Pada Jaringan Komputer

Setiap jaringan komputer pasti memiliki celah-celah keamanan yang dapat diserang. Dalam penelitian yang dilakukan oleh Nugraha (2016:14) mengatakan bahwa bentuk dari ancaman jaringan komputer ditujukan terhadap sumber daya fisik dan logik yang mendukung jaringan yang ada, bentuk ancaman tersebut diantaranya sebagai berikut:

a. DDOS (*Distributed Denial of Service*)

Serangan DOS (*Denial-Of-Service Attacks*) merupakan jenis serangan terhadap sebuah komputer atau server pada jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sehingga komputer tersebut tidak mampu menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang.

Dampak dari serangan DDOS akan mengakibatkan *bandwidth* yang digunakan oleh korban akan habis yang mengakibatkan terputusnya koneksi antar *server*, jika serangan DDOS tidak segera ditanggulangi dapat menyebabkan kerusakan secara permanen terhadap *hardware* maupun *software* korban.

b. *Brute Force Attack*

Serangan *brute-force* merupakan sebuah teknik serangan terhadap sebuah sistem keamanan komputer dengan menggunakan percobaan terhadap semua kunci yang mungkin. Pendekatan ini pada awalnya merujuk pada sebuah program komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia.

Secara sederhana, menebak *password* dengan mencoba semua kombinasi karakter yang mungkin. *Brute force attack* digunakan untuk memasuki akses ke suatu *host* (*server/workstation/network*) atau pada data yang terenkripsi.

c. *Scan*

Menurut Ramesh (2014:51), *scanning* merupakan proses dimana penyerang akan menggali informasi mengenai alamat IP target, sistem operasi yang digunakan, arsitektur jaringan yang digunakan, serta servis yang sedang berjalan pada komputer pun dapat di peroleh. Tidak seperti *footprinting* yang hanya mengali informasi secara pasif dari pihak ketiga dalam berbagai sumber, *scanning* secara aktif berhadapan dengan target untuk menperoleh informasi.

Dalam melakukan scanning, terdapat beberapa tipe scanning diantaranya sebagai berikut :

1) *Port scanning*, meliputi pengiriman beberapa pesan ke komputer target untuk memperoleh tipe servis jaringan apakah yang sedang berjalan pada jaringan tersebut. Dikarenakan servis tersebut berkaitan dengan nomor *port*, sehingga dengan melakukan *port scan* terhadap target akan menampilkan seluruh port yang terbuka.
2) *Network scanning*, merupakan suatu prosedur untuk mengidentifikasi *host* yang sedang aktif pada jaringan target yang bertujuan untuk melakukan serangan pada target ataupun untuk menilai keamanan jaringan. Langkah ini akan memungkinkan penyerang untuk membuat daftar *host-host* yang dapat diserang secara langsung atau menggunakan host tersebut untuk menyerang host lain secara tidak langsung.
3) *Vulnerability scanning*, berhubungan dengan penggunaan *tools* otomastis yang dikenal dengan *vulnerability scanner* yang dengan secara otomatis mengidentifikasi kelemahan-kelemahan keamanan terhadap sistem komputer

di jaringan tersebut. *Tools* ini akan melacak target dan mencari tahu celah keamanan manakah yang dapat di eksploitasi.

d. *Spoofing*, merupakan teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang terkoneksi dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya.

e. *Sniffer*, merupakan ancaman terhadap peralatan yang dapat memonitor proses yang sedang berlangsung.

f. *Remote Attack*, segala bentuk serangan terhadap suatu mesin di mana penyerangnya tidak memiliki kendali terhadap mesin tersebut karena dilakukan dari jarak jauh di luar sistem jaringan atau media transmisi.

8. *Software* Simulasi

Software simulasi yang digunakan untuk menguji jaringan adalah:

a. *PuTTY*

Menurut Andi (2010), *putty* adalah sebuah program *open source* yang mampu digunakan untuk melakukan protokol jaringan SSH, Telnet dan Rlogin. Aplikasi ini merupakan aplikasi *portable* sehingga tidak perlu di *install*. Protokol ini dapat digunakan untuk menjalankan sesi *remote* pada sebuah komputer melalui sebuah jaringan, baik itu LAN, maupun internet. Program ini banyak dipergunakan para pengguna komputer tingkat menengah ke atas, yang biasanya digunakan untuk menyambungkan, mensimulasi, ataupun mencoba berbagai hal yang terkait dengan jaringan.

b. *File Zilla*

FileZilla merupakan salah satu *software* SFTP (*Secure File Transfer Protocol*) gratis, *open source*, *cross-platform*, berlisensi GNU (*General Public Lisence*) yang digunakan untuk melakukan *upload file*/*transfer file* via protokol FTP melalui jaringan internet maupun LAN di komputer. *File* yang di *upload* pun dapat dalam jumlah dan kapasitas besar tanpa harus menggunakan kontrol panel *hosting* secara langsung. Binari FileZilla tersedia untuk Windows, Linux, dan Mac OS X. *Software* ini mendukung FTP, SFTP, dan FTPS (FTP di SSL/TLS).

9. *Firewall*

Firewall adalah sebuah sistem atau perangkat yang bertugas untuk mengatur lalu lintas jaringan komputer yang dianggap aman untuk melewatinya dan mencegah lalu lintas jaringan yang dianggap tidak aman untuk melewatinya (Athailah, 2013:5).

Menurut Suprapto (2020:20), cara kerja *firewall* adalah dengan cara melakukan penyaringan terhadap paket data di dalam jaringan kedalam sebuah tabel, sehingga memudahkan dalam membedakan antara paket data mana yang boleh masuk kedalam jaringan dengan paket data mana yang harus dibuang atau dilarang. Proses ini dilakukan baik pada *Network Layer* dan *Transport Layer*.

10. Monitoring

a. Pengertian Monitoring

Widiastuti dan Susanto (2014), berpendapat bahwa sistem monitoring atau sistem pengawasan merupakan suatu upaya yang sistematik untuk menetapkan kinerja standar pada perencanaan untuk merancang sistem umpan balik informasi, untuk membandingkan kinerja aktual dengan menggunakan standar yang telah ditentukan, untuk menetapkan apakah telah terjadi suatu penyimpangan tersebut, serta untuk mengambil tindakan perbaikan yang diperlukan untuk menjamin bahwa semua sumber daya perusahaan atau organisasi telah digunakan secara efektif dan seefisien mungkin untuk mencapai tujuan perusahaan atau organisasi.

Monitoring juga dapat didefinisikan sebagai langkah untuk mengkaji apakah kegiatan yang dilaksanakan sudah sesuai dengan rencana, mengidentifikasi masalah yang terjadi agar langsung dapat diatasi, melakukan penilaian terhadap pola kerja dan manajemen yang digunakan untuk mencapai tujuan, mengetahui kaitan antara kegiatan dengan tujuan untuk memperoleh ukuran kemajuan.

Sehingga proses monitoring merupakan suatu proses menganalisa dan meninjau ulang perubahan yang terjadi untuk memeriksa terhadap proses berikut objek atau untuk mengevaluasi kondisi ataupun kemajuan menuju tujuan hasil manajemen terhadap efek tindakan dari beberapa jenis antara lain tindakan untuk mempertahankan manajemen yang sedang berjalan.

b. Tujuan Monitoring Jaringan

Tujuan dari monitoring keamanan jaringan adalah untuk mengetahui serta mengumpulkan data yang terjadi pada jaringan sehingga data dari proses monitoring jaringan dapat digunakan untuk mengatur dan mengontrol jaringan. berikut beberapa alasan dilakukannya monitoring:

1. Melakukan pengawasan terhadap konektivitas dan lalu lintas jaringan.
2. Mengetahui masalah yang terjadi pada jaringan.
3. Memberikan laporan masalah yang terjadi ke *administrator* jaringan.

11. *Mikrotik*

Mikrotik merupakan suatu perangkat jaringan berupa *hardware* maupun *software* yang dapat difungsikan sebagai *router*. Produk *hardware* unggulan mikrotik berupa *router, switch, antenna*dan perangkat pendukung lainya, Sedangkan untuk produk *software* unggulan mikrotik merupakan *MikroTik RouterOS.*

a. *Mikrotik Routerboard*

RouterBoard adalah *router embedded* produk dari mikrotik. *RouterBoard* merupakan sebuah pc mini yang terintegrasi karena dalam satu board tertanan prosesor, ram, rom, dan memori flash. *Routerboard* menggunakan os *RouterOS* yang memiliki fungsi sebagai *router* jaringan, *bandwidth management, proxy server, dhcp, dns server* dan dapat juga berfungsi sebagai *hotspot server*.*Routerboard* bisa menjalankan fungsi sebuah *router* tanpa tergantung pada PC lagi, kerena semua fungsi pada sebuah *router* telah ada dalam *routerboard.* Jika dibandingkan dengan pc yang di *instal routerOS, routerboard* ukuranya lebih kecil dan hemat listrik karena hanya mengunakan adaptor. Untuk digunakan pada jaringan *wifi* bisa dipasang di atas *tower* dan menggunakan PoE sebagai sumber arusnya.

Gambar 14. Mikrotik
Sumber: www.mikrotik.com

b. *Mikrotik RouterOS*

Mikrotik OS merupakan OS berbasis *linux* yang diperuntukkan sebagai *network router*, didesain untuk memberikan kemudahan bagi penggunanaya.Administarasinya biasa dilakukan melalui *Windows Application (Winbox)*. *Mikrotik RouterOS* adalah sistem operasi independen berbasis *Linux* khusus untuk komputer yang difungsikan sebagai router. Selain itu *MikroTik* dapat juga berfungsi sebagai *firewall* bagi komputer lain dan memberikan prioritas bagi komputer lain agar bisa mengakses data internet maupun data lokal.

12. *Winbox*

Menurut Ardianto dan Akbar (2016:136), *Winbox* merupakan *utilitas* yang digunakan untuk konektifitas dan konfigurasi *proxy* menggunakan alamat MAC atau protokol IP. *Winbox* dapat dengan cepat dan mudah dikonfigurasikan OS *router mikrotik* menggunakan mode GUI.

Fungsi *winbox* adalah untuk melakukan konfigurasi pada mikrotik secara GUI atau dengan tampilan *desktop, winbox* dapat memudahkan pengguna untuk melakukan *setting mikrotik* karena tidak menggunakan *syntax* ataupun kode perintah secara *console*.

13. *Quality of Service* (QoS)

*Quality of Servic*e merupakan kemampuan suatu jaringan untuk menyediakan layanan yang baik dengan menyediakan kapasitas jaringan internet yang sesuai dengan standar yang ada (Cahyadi, Santoso dan Zahra, 2013).

QoS didesain untuk membantu *end user (client)* menjadi lebih produktif dengan memastikan bahwa *user* mendapatkan performansi yang handal dari aplikasi-aplikasi berbasis jaringan. QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda.

Berikut presentase dan indeks QoS ETSI pada jaringan.

Tabel 1. Nilai, Indeks dan Kategori Standar QoS ETSI

Nilai	Persentase (%)	Indeks
3,8-4	95-100	Sangat Bagus
3-379	75-94,75	Bagus
2-2,99	50-74,75	Sedang
1-1,99	25-49,75	Buruk

Sumber: ETSI

14. Parameter Qos

a. *Throughput*

Menurut (Iskandar & Hidayat, 2015) *throughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada *destination* selama *interval* waktu tertentu dibagi oleh durasi *interval* waktu tersebut.

Perhitungan nilai *troughput* dirumuskan sebagai berikut :

$$Throughput = \frac{\text{Paket Data yang Diterima}}{\text{Waktu Pengiriman Data}} \text{ x } 8$$

Tabel 2. Nilai,Indeks dan kategori *Throughput*

Kategori *Throughput*	*Troughput* (bps)	Indeks
Sangat Bagus	76-100	4
Bagus	51-75	3
Sedang	26-50	2
Buruk	< 25	1

Sumber: ETSI

b. *Packet Loss*

Packet loss adalah parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket data yang hilang pada saat melakukan transmisi data di dalam jaringan.

Perhitungan nilai *packet loss* dirumuskan sebagai berikut:

$$Packet\ Loss = \frac{\text{(Total Paket Data Dikirim – Total Paket Data Diterima)}}{\text{Total Paket Data Dikirim}} \text{ x } 100\%$$

Secara umum terdapat empat ketegori penurunan kualitas jaringan berdasarkan nilai *packet loss* sesuai dengan versi *TIPHON* (*Telecommunications and Internet Protocol Harmonization Over Network*), standarisari nilai *packet loss* sebagai berikut:

Tabel 3. Nilai, Indeks dan Kategori *Packet Loss*

Kategori *Packet Loss*	*Packet Loss*	Indeks
Sangat bagus	0	4
Bagus	3%	3
Sedang	15%	2
Jelek	25%	1

Sumber: ETSI

c. *Delay*

Delay atau keterlambatan adalah sebuah kondisi dimana terjadi selisih waktu antara waktu paket diterima dan waktu pengirimannya. *Delay* merupakan waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan.

Perhitungan nilai *delay* dirumuskan sebagai berikut:

$$delay = \frac{\text{Total } Delay}{\text{Total Paket Data Diterima}}$$

Menurut versi *TIPHON* (*Telecommunications and Internet Protocol Harmonization Over Network*) standarisari nilai *latency/delay* sebagai berikut.

Tabel 4. Nilai, Indeks dan Kategori *Delay*

Kategori *Delay*	*Delay*	Indeks
Sangat bagus	< 150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	300 s/d 450 ms	2
Jelek	> 450 ms	1

Sumber: ETSI

d. *Jitter*

Jitter merupakan variasi *delay* (perbedaan selang waktu) antar paket yang terjadi pada jaringan, yang disebabkan oleh panjangnya antrian pada saat pengolahan data yang terjadi pada jaringan. *Jitter* juga didefinisikan sebagai gangguan pada komunikasi digital maupun analog yang disebabkan oleh perubahan sinyal karena referensi posisi waktu.

Perhitungan nilai *jitter* dirumuskan sebagai berikut:

$$Jitter = \frac{\text{Total Variasi } Delay}{\text{Total paket data Diterima}}$$

Secara umum terdapat empat ketegori penurunan kualitas jaringan berdasarkan nilai *jitter* sesuai dengan versi *TIPHON* (*Telecommunications and Internet Protocol Harmonization Over Network*), standarisasi nilai *jitter* sebagai berikut:

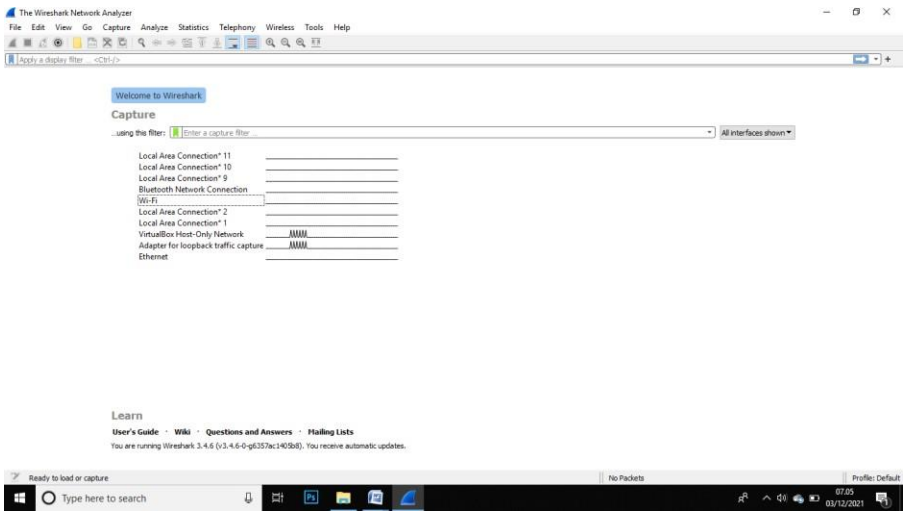
Tabel 5. Nilai, Indeks dan Kategori *Jitter*

Kategori *Jitter*	*Jitter*	Indeks
Sangat bagus	0 ms	4
Bagus	0 s/d 75 ms	3
Sedang	76 s/d 125 ms	2
Jelek	125 s/d 225 ms	1

15. *Wireshark*

Menurut Putra (2018), Wireshark merupakan *tool* yang ditujukan untuk melakukan penganalisisan paket data jaringan. Wireshark juga melakukan pengawasan paket secara *real time* dan kemudian menangkap data dan menampilkannya selengkap mungkin. Wireshark memiliki beberapa fitur yang tersedia untuk sistem operasi *linux* dan *windows*, menangkap paket data dari antarmuka jaringan, *wireshark* juga dapat menangkap lalu lintas dari banyak jenis media jaringan yang berbeda.

Menurut Ariyus 2006 (dalam Diansyah, 2015), Wireshark merupakan aplikasi untuk melakukan analisa aktivitas jaringan komputer yang memiliki fungsi-fungsi yang berguna bagi profesional jaringan, administrator, peneliti, hingga pengembang piranti lunak jaringan. *Tool* ini mampu bekerja secara *real time* dalam menangkap paket-paket data/informasi yang berjalan dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa menggunakan aplikasi wireshark.



Gambar 15. Tampilan *Interface* Wireshark
Sumber: Hasil Dokumntasi Penulis

16. Notifikasi

Notifikasi merupakan pemberitahuan berupa kabar, informasi dan sebagainya. Notifikasi yang berkaitan terhadap sebuah sistem dapat diartikan merupakan sebuah pemberitahuan yang dapat diberikan suatu sistem kepada pengguna baik melalui email, ponsel, maupun internet. Notifikasi dapat berupa pemberitahuan yang berisi teks kata, gambar, video, maupun suara.

17. Telegram

Telegram merupkan sebuah aplikasi *messenger* berbasis *cloud* dengan sinkronisasi yang mulus. Hasilnya, *user* dapat mengakses pesan dari beberapa perangkat sekaligus, termasuk tablet dan komputer, dan berbagi foto, video, dan *file* dalam jumlah tak terbatas (dokumen, zip, mp3, dll) masing-masing hingga 2 Gb.API dan kode Telegram terbuka, dan pengembang dipersilakan untuk membuat aplikasi Telegram mereka sendiri. Telegram juga memiliki Bot API, *platform* untuk pengembang yang memungkinkan siapa saja dengan mudah membuat alat khusus untuk Telegram, mengintegrasikan layanan apa pun, dan bahkan menerima pembayaran dari pengguna di seluruh dunia (Telegram, 2020).

2.2 Hasil Penelitian Relevan

Beberapa hasil penelitian yang relevan yang dapat dijadikan sebagai perbandingan penelitian yang akan dilakukan penulis yaitu:

1. Marta, Hartawan dan Satwika (2020) dengan judul "Analis Sistem Monitoring Keamanan *Server* Dengan SMS *Alert* Berbasis Snort", pada penelitian ini penulis menggunakan teknik pengumpulan data sekunder dengan mempelajari, meneliti, dan mencari berbagai sumber buku dan jurnal ilmiah. Pada penelitian ini dibangun sebuah sistem keamanan *server* yang dapat melakukan monitoring pada sebuah *server* ketika terdeteksi adanya aktifitas yang tidak wajar. Pemberitahuan akan dikirimkan melalui SMS (*Short Message Service*) ke *handphone administrator* jaringan. Sistem yang dibangun melakukan pendeteksian intrusi pada *server* secara *realtime* menggunakan Snort. Perbedaan antara penelitian ini dan penelitian yang akan dilakukan oleh penulis adalah penelitian ini akan menggunakan telegram sebagai sistem notifikasi, dan akan fokus pada pengimplementasian sistem serta proses monitoring mengenai kinerja jaringan, melakukan analisa lalu lintas jaringan.
2. Suhartono (2017) dengan judul "Sistem Pengamanan Jaringan Admin Server Dengan Metode *Intrusion Detection System* (IDS) Snort Menggunakan Sistem Operasi Clearos" pada penelitian ini penerapan sistem IDS menggunakan percobaan terhadap *traffic* jaringan server laboratorium secara langsung dengan beberapa parameter yaitu *FTPBruteforce* dan

SSHBruteforce, pengujian sistem di lakukan bertahap yang terdiri dari pengujian *Email (Email Server)* dan sistem IDS. Perebedaan antara penelitian ini dan penelitian yang penulis akan lakukan terletak pada metode yang diterapkan dalam proses pengamanan jaringan. Penelitian yang akan dilakukan akan menggunakan *software* monitoring berupa wireshark serta penulis akan menganalisis dan mengimplementasikan proses monitoring pada sistem yang diterapkan oleh instansi terkait.

3. Susanto dan Rachmawati (2018) dengan judul "Implementasi dan Analisis Jaringan Menggunakan *Wireshark, Chain and Abels, Network Minner* (Studi Kasus: AMIK Dian Cipta Cendekia)". Penelitian ini bertujuan agar dapat memonitoring penggunaan jaringan sehingga dapat mengetahui situs apa saja yang dibuka oleh mahasiswa yang terhubung pada jaringan AMIK Dian Cipta Cendikia Bandar Lampung dalam mengakses internet. Metode Penelitian yang digunakan dalam penelitian ini adalah dengan menggunakan Studi Kasus, Studi Kasus menggunakan cara-cara yang sistematis dalam melakukan pengamatan, pengumpulan data, analisis informasi, dan pelaporan hasilnya, pengamatan terhadap interaksi paket data dilakukan menggunakan Software Wireshark, Cain and Abels dan NetworkMiner. Hasil yang diperoleh pada penelitian ini adalah penggunaan *wifi* belum dimanfaatkan secara penuh oleh mahasiswa dengan baik dikarenakan banyak mahasiswa yang menggunakannya untuk mengakses social media.

2.3 Kerangka Pikir

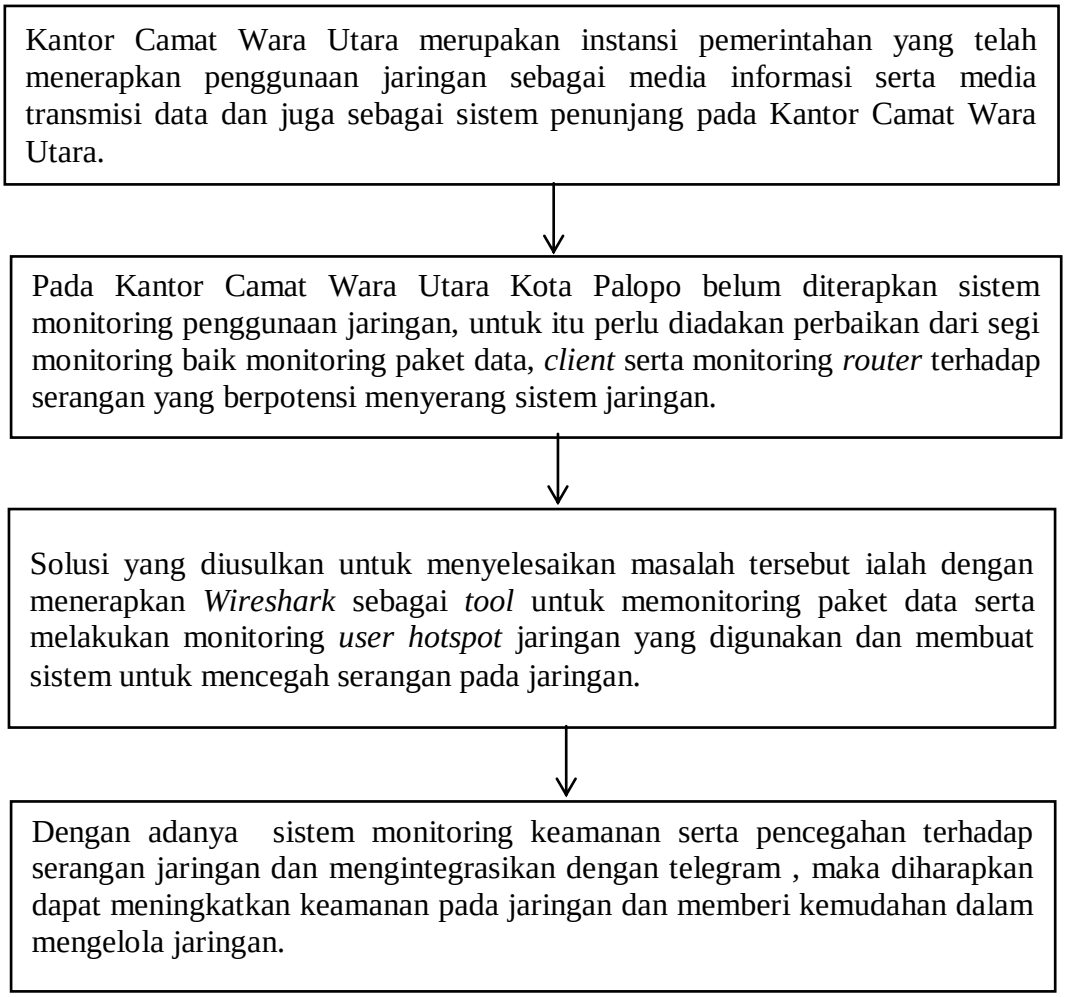
Perkembangan teknologi pada saat ini begitu cepat, di iringi denga banyak kemudahan yang didapatkan. Salah satu bentuk pengembangan jaringan komputer adalahinternet, kemudahan sarana komunikasi dan informasi yang diberikan internetmenjadikan internet salah satu hal yang sangat penting di setiap instansi.

Kantor Camat Wara Utara saat ini telah memanfaatkanperkembangan teknologi yang semakin pesat dan menjadiperan penting terhadap instansi tersebut dalam melakukan beberapa pekerjaanyang berhubungan dengan *internet.*

Salahsatu permasalahan yang ada pada Kantor Camat Wara Utara adalah belum adanya sistem monitoring untuk paket data pada jaringan tersebut serta

belum adanya sistem untuk memonitoring serangan yang sewaktu-waktu dapat menyerang jaringan tersebut. Dengan diusulkannya penggunaan mikrotik memberikan solusi dalam memonitoring serangan terhadap jaringan komputer.

Untuk memperjelas masalah yang akan disajikan, maka berikut akan ditunjukkan kerangka pikir sebagai berikut ini:



Gambar 16. Kerangka Pikir