BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada saat ini isu keamanan jaringan menjadi sangat penting dan patut untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para *hacker*, baik jaringan *wired* LAN maupun *wireless* LAN. Pada saat data dikirim akan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk menyadap atau mengubah data tersebut. Dalam pembangunan perancangannya, sistem keamanan jaringan yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para *hacker.* (Nugroho, 2012).

Secara terus menerus mengalami perkembangan luar biasa sebab teknologi informasi memiliki pengaruh yang semakin tinggi terhadap bagaimana kita bekerja, berkomunikasi, berbelanja dan menikmati hiburan. Program *online* dalam keamanan komputer meliputi dua bidang spesialisasi utama: Pertama, keamanan jaringan yang meliputi perlindungan jaringan IT dari para *hacker*, kehilangan data, pencurian identitas, virus dan jenis serangan *malware* lainnya.

Keamanan jaringan dikatakan aman apabila meningkatakan keamanan jaringan dengan pengamanan secara fisik, meningkatkan keamanan jaringan dengan pengamanan akses, pengamanan data, meningkatkan keamanan jaringan dengan pengamanan komunikasi jaringan. Selain itu, juga menggunakan enskripsi pada akses nirkabel, mengganti alamat SSID, mematikan fitur *interface* atau antarmuka *router*, mengganti anti virus dan melakukan *backup*. Sedangkan keamanan jaringan dikatakan tidak aman apabila terjadi serangan dengan model *Interception*, *Intteruption*, *Fabrication* dan *Modification*.

Forensik komputer yang meliputi investigasi terhadap kejahatan internet, seperti pencurian identitas, penyalahgunaan hak milik orang lain, pornografi anak-anak di bawah umur dan pengintaian lewat internet. Secara khusus dan mendalam masalah proses penemuan, pengumpulan dan analisis bukti-bukti digital dari

berbagai sumber seperti *hard drive* komputer dan email dan penyiapan bukti-bukti untuk melakukan penuntutan kejahatan komputer. Perlu kita sadari bahwa untuk mencapai suatu keamanan itu adalah suatu hal yang sangat mustahil, seperti yang ada dalam dunia nyata sekarang ini. Tidak ada satu daerah pun yang betul-betul aman kondisinya, walau penjaga keamanan telah ditempatkan di daerah tersebut, begitu juga dengan keamanan sistem komputer, namun yang bisa kita lakukan adalah untuk mengurangi gangguan keamanan tersebut. (Sulianta, 2016).

Kejahatan-kejahatan tersebut dapat dicegah dengan menggunakan metode Model Proses Forensik karena Model Proses Forensik adalah kegiatan menangkap, mencatat dan menganalisis kejadian pada jaringan untuk menemukan sumber serangan keamanan atau malasah kejadian lainya. Kekuatan forensik ada pada pengumpulan dan menganalisis data dari berbagai sumber daya komputer seperti *log* antivirus, *log database* atau *log* dari aplikasi yang digunakan sistem pendeteksi serangan dapat menggunakan *tools Instrusion Detection System* (IDS) Snort. *Snort* merupakan IDS yang berbasis *open source*. Pada Model Proses Forensik, *Snort* digunakan untuk menganalisis semua lalu lintas jaringan untuk menyadap dan mencari jenis penyusupan dalam sebuah jaringan. (Singh, 2009)

Kantor Dinas Pendidikan Kota Palopo, merupakan salah satu instansi yang di Kota Palopo memiliki jaringan internet yang luas dimana jaringan internet tersebut rentan terhadap serangan jaringan, karena jaringan kantor belum menerapkan sebuah sistem keamanan jaringan. Maka dari itu jaringan di Kantor Dinas Pendidikan Kota Palopo dapat di salahgunakan oleh masyarakat luar yang banyak mengakses jaringan internet mengakibatkan munculnya beberapa masalah ketika jaringan tersebut digunakan yaitu koneksi jaringan lambat. Sejauh ini belum terdapat sistem keamanan yang dapat melakukan analisis, sehingga serangan yang terjadi dapat mengganggu kecepatan jaringan pada *server*.

Melihat permasalahan diatas pada Kantor Dinas Pendidikan Kota Palopo membutuhkan sebuah sistem keamanan jaringan pada jaringan instansi untuk menghindari serangan dari pihak luar yang tidak bertanggung jawab. Hal tersebut dilakukan supaya semua pengguna internet bisa melakukan akses jaringan merasa aman didalam menggunakan internet. Sehingga dirancang keamanan jaringan

komputer menggunakan model forensik untuk dapat mengetahui serangan terhadap jaringan kantor.

Dari uraian diatas maka penulis sangat tertarik untuk melakukan penelitian dalam hal implementasi keamanan jaringan pada Kantor Dinas Pendidikan Kota Palopo. Sehubungan dengan hal tersebutlah penulis untuk melakukan penelitian yang berjudul "Implementasi Keamanan Jaringan Komputer Dengan Menggunakan Model Forensik pada Kantor Dinas Pendidikan Kota Palopo", sehinggga dapat untuk membantu instansi dalam mengamankan jaringan komputer kepada masyarakat dan pegawai yang ada di Kantor Dinas Pendidikan Kota Palopo.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disebutkan di atas maka dapat dirumuskan permasalahnnya yaitu bagaimana mengimplementasikan model forensik pada jaringan komputer di Kantor Dinas Pendidikan Kota Palopo?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dikemukakan di atas maka tujuan penelitian yang akan dilakukan adalah untuk mengimplementasikan model forensik pada jaringan komputer di Kantor Dinas Pendidikan Kota Palopo.

1.4 Manfaat Penelitian

Dari hasil penelitian diharapkan dapat memberikan manfaat masing-masing kepada:

1. Manfaat bagi dunia akademik

Diharapkan dari hasil penelitian ini akan memberikan suatu referensi yang berguna dalam perkembangan dunia akademik khususnya dalam penelitian-penelitian yang akan datang. Dapat pula memberikan sumbangan pemikiran bagi perkembangan teknologi informasi dalam dunia ilmu pengetahuan.

2. Manfaat bagi mahasiswa

Merupakan studi kasus yang baru dalam menganalisis topologi jaringan yang diperoleh selama duduk di bangku kuliah dan sebagai pembekalan dalam menghadapi dunia kerja yang syarat dengan dunia teknologi informasi.

3. Manfaat bagi Kantor Dinas Pendidikan Kota Palopo

Agar dapat mengetahui sistem keamanan jaringan di Kantor Dinas Pendidikan Kota Palopo apakah sudah aman dari serangan pihak luar yang tidak bertanggungjawab dan dapat memberikan keamanan kepada masyarakat dan pegawai yang ada di Kantor Dinas Pendidikan Kota Palopo.

1.5 Batasan Penelitian

Untuk menghindari ruang lingkup yang terlalu luas sehingga penelitian dapat terarah dengan baik, sesuai tujuan penelitian serta dengan adanya keterbatasan waktu pengerjaan maka perlu adanya batasan penelitian. Batasan penelitian ini adalah sebagai berikut:

1. Penelitian ini berfokus pada pengimplementasian proses model forensik pada jaringan komputer di Kantor Dinas Pendidikan Kota Palopo.
2. Mengimplementasikan proses model forensik pada jaringan komputer di Kantor Dinas Pendidikan Kota Palopo.
3. Teknik pengujian menggunakan Model forensik.
4. Hasil yang di tampilkan berupa keamanan jaringan pada instansi pemerintah yaitu di Kantor Dinas Pendidikan Kota Palopo.

BAB II
TINJAUAN PUSTAKA

2.1 Kajian Teori

Kajian teori berisi topik-topik yang akan dibahas dalam penelitian ini. Landasan teori ini mempunyai peranan penting dalam hal melakukan penelitian kuantitatif. Dengan kajian teori, peneliti dapat menjustifikasi adanya masalah penelitian dan mengindentifikasi arah penelitian.

1. Pengertian Implementasi

Wahab (2016) implementasi adalah sebuah tindakan yang dilakukan oleh seseorang atau sekelompok orang berdasarkan atas kebijakan yang telah ditetapkan sebelumnya. Tindakan tersebut dilakukan atas dasar perencanaan yang jelas serta memiliki tujuan yang jelas pula untuk suatu kegiatan yang direncanakan secara bersama-sama.

Implementasi adalah perluasan aktivitas yang saling menyesuaikan proses interaksi antara tujuan dan tindakan untuk mencapainya serta memerlukan jaringan pelaksana, birokrasi yang efektif. (Setiawan, 2004:39).

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

Harsono (2002:67) mengemukakan pendapatnya mengenai implementasi atau pelaksanaan sebagai berikut: implementasi adalah suatu proses untuk melaksanakan kebijakan menjadi tindakan kebijakan dari politik ke dalam administrasi polituk. Pengembangan kebijakan dalam rangka penyempurnaan suatu program untuk mencapai suatu tujuan.

Busten (dalam Purwaningrum, Purwanto & Darmadi, 2018) Firewall didefinisikan sebagai sebuah komponen atau kumpulan komponen yangmembatasi akses antara sebuah jaringanyang diproteksi dan internet, atau antara kumpulan-kumpulan jaringan lainnya Firewall merupakan solusi untuk mengatasi keamanan di dalam dunia internet baik itu keamanan komputer maupun keamanan jaringan yang banyak dipenuhi dengan berbagai ancaman baik dari dalam maupun dari luar. Dengan suatu konfigurasi yang tepat pada firewall maka

kemungkinan untuk mengamankan suatu data atau komputer pada jaringan menjadi jauh lebih aman.

Ihsana & Maslan (2020) Loic (Low Orbit Ion Cannon) merupakan sebuah tool atau aplikasi peretas jaringan atau open source stress testing, loic sering digunakan untuk serangan DDoS. Pada sebelumnya aplikasi loic di namai Ion Cannon dan sekarang berubah nama menjadi Loic. Loic awalnya di kembangkan oleh Praetox Technologies, namun aplikasi ini kemudian di sebar luaskan pada publik domain. Akhir-akhir ini loic menjadi populer semenjak serangan-serangan yang dilakukan hacktivitis Anonymous pada beberapa web besar. Anonymous sendiri sering menggunakan loic dalam operasinya, dan tentu saja ditambah dengan tool-tool lain dan teknik-teknik tersendiri yang hanyamereka sendiri yang tau.

Oleh karena itu, berdasarkan pengertian impelementasi di atas, dapat disimpulkan bahwa implementasi adalah sebuah tindakan yang dilakukan berdasarkan atas kebijakan yang telah ditetapkan sebelumnya. Tindakan tersebut dilakukan atas dasar perencanaan yang jelas serta memiliki tujuan yang jelas antara tujuan dan tindakan untuk mencapainya serta memerlukan jaringan pelaksana.

2. Keamanan Jaringan

Menurut Ma'sum (2017), keamanan jaringan merupakan sebuah proses pencegahan dan identifikasi dari aktifitas penggunaan yang tidak sesuai jaringan komputer tersebut. Keamanan jaringan juga bertujuan mengantisipasi ancaman dalam bentuk logika maupun fisik yang mengganggu secara langsung dan tidak langsung. Berikut ini adalah 3 konsep umum dalam keamanan jaringan:

1. Resiko

Resiko atau tingkat bahaya untuk menyatakan berapa besar sebuah kemungkinan jika jaringan komputer tersebut disusupi oleh *intruder* atau penyusup.

2. Threat

Untuk menyatakan ancaman yang datang dari pihak yang ingin mengakses sistem jaringan komputer pengguna secara illegal.

3. Vulnerability

Untuk menyatakan seberapa tahan dan kuat sebuah sistem keamanan dari ancaman dan bahaya eksternal yang akan datang.

Tujuan keamanan jaringan dapat dicapai dengan suatu metode keamanan jaringan yang dapat melindungi sistem baik dari dalam maupun luar jaringan, tidak hanya melindungi jaringan tetapi dapat bertindak apabila terjadi serangan yang ada di dalam jaringan. Salah satu metode tersebut yaitu *Intrusion Detection System* (IDS).

3. Jaringan Komputer

Samsumar dan Hadi (2018:1) jaringan komputer adalah sebuah jaringan yang terdiri dari dua komputer yang saling terhubung dengan sebuah media sehingga komputer-komputer tersebut dapat saling berbagi *resource* dan saling berkomunikasi. Kenyataannya sebuah *network* biasanya terdiri dari banyak komputer (lebih dari dua). Jaringan komputer muncul dari adanya kebutuhan untuk berbagi data diantara para pengguna dan memiliki kemampuan dalam memproduksi beberapa jenis informasi yang berupa data, *spreadsheet* atau grafik. Sedangkan konsep dari komputer-komputer yang saling berbagi *resource* dikenal dengan istilah *networking*.

Limbunna (2015:5) jaringan komputer merupakan penggabungan beberapa teknologi komputer dan komunikasi yang merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya bersama untuk mecapai suatu tujuan tertentu.

Jadi jaringan komputer adalah sebuah jaringan yang terdiri dari beberapa komputer yang saling terhubung yang saling berbagi *resource* yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya bersama untuk mecapai suatu tujuan tertentu.

4. Forensik

Sulianta (2016) forensik (berasal dari bahasa Latin *forensic* yang berarti “dari luar”, dan serumpun dengan kata *forum* yang berarti “tempat umum”) adalah bidang ilmu pengetahuan yang digunakan untuk membantu proses penegakan keadilan melalui proses penerapan ilmu atau sains. Ilmu forensik adalah ilmu yang mempelajari benda-benda yang berhubungan dengan kejahatan. Ilmu forensik adalah cara atau metode ilmiah untuk mengumpulan, memeriksa,

menyelidiki informasi yang sudah lewat. Benda-benda ini dinamakan barang bukti. Para ilmuwan forensik mempelajari barang bukti supaya bisa dijadikan sebagai bukti dalam persidangan. Istilah forensik berarti. “dapat dipakai dalam persidangan hukum”.

Pada saat menganalisis barang bukti, para ilmuwan forensik melakukan kegiatan-kegiatan yang sama seperti yang dilakukan para ilmuwan lain: mereka mengamati, menggolongkan, membandingkan, menggunakan angka, mengukur, memperkirakan, menafsirkan data dan kemudian menarik kesimpulan yang masuk akal berdasarkan barang bukti yang ada. Ilmu forensik bersifat aktif dan tak kenal lelah. Dalam kelompok ilmu-ilmu forensik ini dikenal antara lain ilmu fisika forensik, ilmu kimia forensik, ilmu psikolog forensik, ilmu kedokteran forensik, ilmu toksikologi forensik, ilmu psikiatri forensik, komputer forensik dan sebagainya.

Sulianta (2013) berbagai fakta dan bukti tersembunyi untuk ditemukan misalnya: darah, struktur gigi, riwayat kesehatan, sidik jari dan lainnya. Di analisa sedemikian rupa, sehingga didapat fakta yang layak untuk diajukan sebagai pembuktian. Serangkaian proses ini dikenal dengan istilah forensik. Komputer forensik mencakup banyak hal yang harus di pertimbangkan, karenakan ilmu baru yang di bangun karena kebutuhan dan didasari pada kompleksitasi. Ada tiga hal yang perlu dipehatikan dalam menerapkan forensik secara umum, antara lain: prinsip *pyolic*/Kebijakan dan Prosedur.

Prinsip pada praktekya melibatkan peralatan *(special tools andequipment*) untuk mengumpulkan *elektronik evidence*. Yang penting bukan *tools*-nya, tetapi keahlian yang sudah teruji lewat pengalaman. Bahkan *tools* akan disesuaikan berdasarkan cara kerja nantinya (Sulianta, 2013).

Sulianta (2013) prosedur dan metode (*Procedure*): harus dirancang sedemikian rupa terhadap peralatan dan mendapatkan/ mengumpulkan *electronik evedence*. Kebutuhan akan peralatan dan perangkat dialamati oleh aspek dari proses yang mencakup: pengumpulan *(collection*), pengemasan *(packaging*), dan pengiriman (*transpotation*). Ketiga hal utama tadi dilaksanakan dengan berbagai peralatan yang tidak hanya komputer. Perangkat-perangkat forensik pada umumnya (*general crime scene processing tools*) mungkin digunakan dalam

komputer forensik, sebagai cara pemberlakuan terhadap suatu bukti, misalnya seperti digunakan.

Farhat (2008) komputer forensik kadang dikenal sebagai ilmu komputer forensik adalah cabang dari ilmu forensik digital yang berkaitan dengan bukti yang ditemukan di komputer dan media penyimpanan digital. Tujuan dari komputer forensik adalah untuk memeriksa media digital dengan tujuan mengidentifikasi, melestarikan, memulihkan, menganalisis dan menyajikan fakta dan opini tentang informasi digital. Disipin ilmu yang melibatkan teknik yang sama dan prinsip-prinsip untuk pemulihan data, tetapi dengan pedoman tambahan dan praktek yang dirancang untuk membuat hukum jejak audit. Bukti dari investigasi forensik komputer biasanya tunduk pada pedoman dan praktik dari bukti digital lain yang sama.

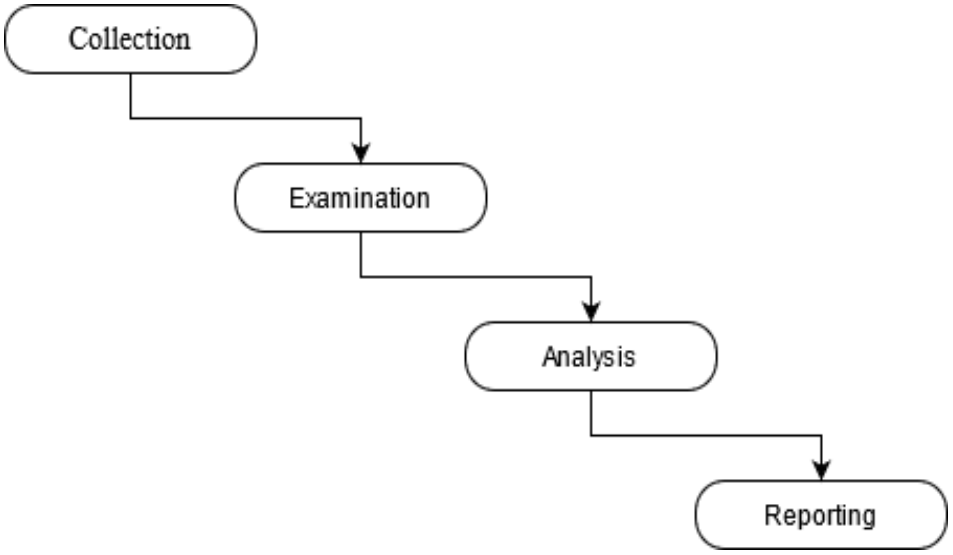
Adapun manfaat dan tujuan forensik yaitu: Tujuannya ialah untuk mengamankan dan menganalisis bukti digital serta memperoleh berbagai fakta yang objektif dari sebuah kejadian atau pelanggaran keamanan dari sistem informasi. Contohnya, melalui Internet Forensik, kita dapat megetahui siapa saja orang yang mengirim email kepada kita, kapan dan dimana keberadaan pengirim. Dalam contoh lain kita bisa melihat siapa pengunjung *website* secara lengkap dengan informasi IP *Address*, komputer yang dipakainya dan keberadaannya serta kegiatan apa yang dilakukan pada *website* kita tersebut.

a. Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang dibutuhkan.
b. Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut, dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir.
c. Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer.
d. Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.

Adapun tujuan forensik yaitu:

a. Untuk membantu memulihkan, menganalisa dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa hingga dapat dipergunakan sebagai alat bukti sah dipengadilan.

b. Untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud.



Gambar 1. Model Forensik
(Sumber : Media.neliti.com)

Tahapan penelitian pada gambar 1. yaitu:

1. Tahap Pengkoleksian (*Collection*): Pada tahap ini yang dilakukan meneliti dan mencari bukti-bukti, pengenalan terhadap bukti-bukti penyusupan dan pengumpulan bukti.
2. Tahap Pemeriksaan (*Examination*): Pada tahap ini, pencarian informasi yang tersembunyi dan mengungkapkan dokumentasi yang relevan.
3. Tahap analisis (*Analysis*): Telihat pada hasil pemeriksaan untuk nilai pembuktian pada kasus yang ada. Tahap ini digunakan untuk menjawab pertanyaan forensik yaitu serangan apa yang terjadi, IP siapa yang melakukan serangan, kapan serangan itu terjadi, dimana serangan itu terjadi, bagaimana serangan tersebut bisa terjadi dan mengapa itu terjadi.

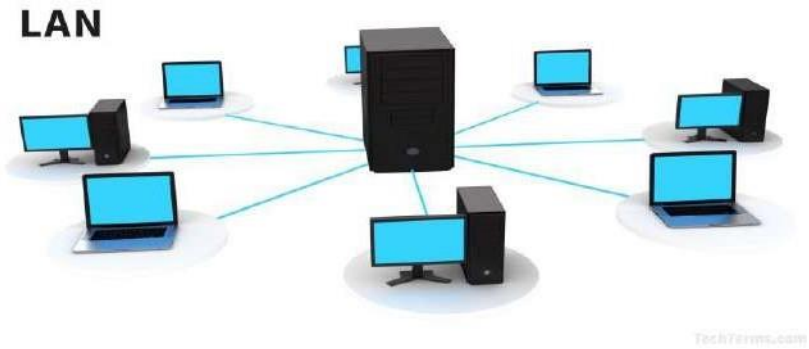
4. Tahap pelaporan (*Reporting*): Penulisan laporan mengenai proses pemeriksaan dan data yang diperoleh dari semua penyelidikan.

5. Jenis Jaringan Komputer

Menurut Gunawan, Simorangkir dan Ghiffari (2018), ada 4 jenis jaringan komputer, yaitu:

a. *Local Area Network* (LAN)

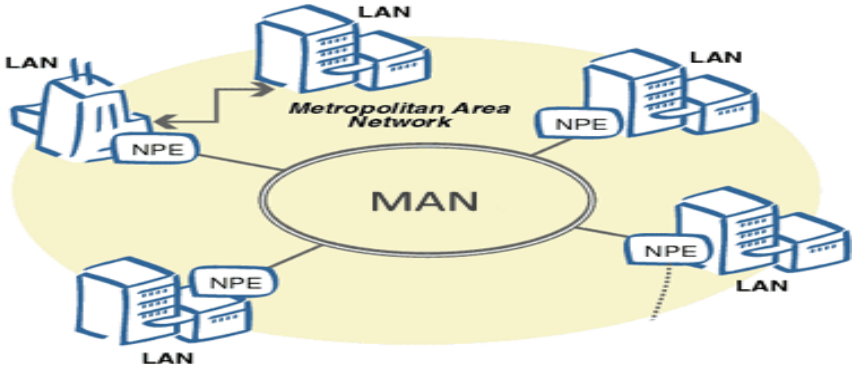
LAN adalah jaringan yang dibatasi oleh area yang relatif kecil, umumnya dibatasi oleh area lingkungan seperti sebuah perkantoran di sebuah gedung atau sebuah sekolah dan tidak jauh dari sekitar 1 km persegi.



Gambar 2. *Local Area Network* (LAN)
(sumber: Ennes Blog – WordPress.com)

b. *Metropolitan Area Network* (MAN)

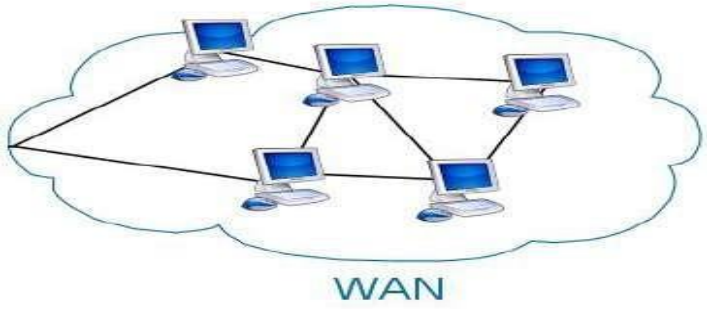
MAN meliputi area yang lebih besar dari LAN, misalnya antar wilayah dalam satu provinsi. Dalam hal ini jaringan menghubungkan beberapa buah jaringan-jaringan kecil ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu jaringan bank dimana beberapa kantor cabang sebuah bank di dalam sebuah kota besar dihubungkan antara satu dengan lainnya.



Gambar 3. *Metropolitan Area Network* (MAN)
(Sumber: GuruPendidikan.com)

c. *Wide Area Network* (WAN)

WAN adalah jaringan yang lingkupnya sudah menggunakan media satelit atau kabel bawah laut, sebagai contoh keseluruhan jaringan bank yang ada di Indonesia atau yang ada di negara-negara lain.



Gambar 4. *Wide Area Network* (WAN)
(Sumber: Welcomtomyblog)

d. *Wireless Local Area Network* (WLAN)

WLAN adalah jaringan komputer yang menggunakan gelombang sinyal radio sebagai transmisi data. Data ditransfer dari satu perangkat ke perangkat yang lain tanpa menggunakan kabel sebagai perantara.

Gambar 5. *Wireless Local Area Network* (WLAN)
(Sumber: The Tech Terms Computer Dictionary)

6. Pengertian OSI *Layer*

Arsitektur jaringan model *Open Systems Interconnection* (OSI) memiliki beberapa *layer* untuk memproses pertukaran data dalam sistem yang berlainan melalui *hierarki* atau tingkatan protokol komunikasi yang dibagi menjadi tujuh *layer*, yaitu:

1) *Layer* 1–*Physical*

Menurut kristanto (2003), *layer* ini secara fisik terkoneksi satu dengan yang lain dan menyediakan transmisi aktual dari informasi melalui media, baik *wired* maupun *wireless*. *Layer* ini merupakan aliran dari bit (*binary* digit 1 dan 0) berupa detak elektris, sinyal radio atau sinar cahaya yang melalui jaringan pada level

elektrikal dan *mekanikal*. *Layer* ini merupakan *layer* secara *hardware* bertugas untuk mengirim dan menerima data pada sisi pembawa (*carier*) termasuk pengkabelan, kartu, bentuk port koneksi serta aspek fisik lainnya *Layer* 2–Data *link*

Sedangkan menurut Kuswayanto (2008), pada *layer* ini paket-paket data akan dienkode dan didekode menjadi susunan bit-bit. Data tersebut dipecah menjadi *frame-frame* data, kemudian ditransmisikan dan diurutkan. Selanjutnya, pengaturan sinkronisasi *frame* akan diproses jika terjadi kesalahan baik pada pengirim maupun penerima.

Layer data *link* terbagi menjadi dua *sublayer*, yaitu:

a) *Media Access Control* (MAC) yang mengatur bagaimana komputer dijaringan mendapatkan akses data untuk kemudian melakukan proses transmisi.

b) *Logical Link Control* (LLC) yang mengatur sinkronisasi *layer*, aliran data dan melakukan pemeriksaan apabila terjadi kesalahan.

2) Layer 3*–Network*

Layer ini menyediakan proses penentuan *rute* paket di jaringan dari pengirim ke penerima. *Layer* ini juga menyediakan beberapa teknologi untuk melakukan *switching* dan *routing*, membuat *path* secara logika yang disebut virtual dan melakukan transmisi data dari *node* ke *node*. Proses *routing* berguna untuk memastikan paket data tersebut terkirim pada arah yang benar untuk tujuan tertentu. Protokol seperti *Internet Protocol* (IP) beroperasi pada *layer* ini. Selain proses *routing*, proses yang dilakukan oleh *layer* ini adalah proses *forwarding*, metode pegalamatan, *internetworking*, penanganan kesalahan, mengontrol tabrakan data dan proses pengurutan paket.

3) Layer 4*-Transport*

Layer ini juga disebut *layer host to host* atau *end to end*, artinya *layer* ini menyediakan proses transfer data secara transparan antara *end system* (*host*) serta bertanggung jawab terhadap metode *recovery* kesalahan *end to end*. *Layer* ini juga mempunyai fungsi sebagai pengatur aliran data serta selalu memastikan kelengkapan data saat dilakukan proses transfer. Contoh protokol yang beroperasi pada *layer* ini adalah *Transmision Cntrol Protocol* (TCP).

4) *Layer* 5–*Session*

Layer ini berfungsi untuk membantuk, mengatur, dan menghentikan koneksi antara aplikasi. *Layer* ini akan mengatur koordinasi, menghentikan percakapan antar sistem, pertukaran data dan dialog antar aplikasi (Lukas and Jonathan 2006).

5) *Layer* 6–*Presentation*

Layer ini bertugas melakukan negosiasi *sintaks-sintaks* transfer data untuk *layer* aplikasi dan berfungsi sebagai penerjemah diantara data format yang berlainan. *Layer* ini akan melakukan pengkodean untuk mewakili data saat berkomunikasi pada sistem yang dikembangkan oleh *vendor* yang berlainan, sehingga *layer* dan enkripsi data akan dikrimkan melintasi jaringan tanpa harus selalu mempertimbangkan permasalahan kompatibilitas.

6) *Layer* 7-*Application*

Layer ini menyediakan komunikasi antara *user* dengan layanan komunikasi standar seperti transfer dan *e-mail*. Beberapa *software* yang berjalan di atas *layer* ini adalah HTTP (*HyperText Transfer Protocol*), FTP (*File Transfer Protocol*), SMTP (*Send Mail Transfer Protocol*), dan NFS (*Network File System*).

7. Pengertian *Mikrotik*

Herlambang (2008) *mikrotik*ls atau yang lebih di kenal dengan *mikrotik* didirikan tahun 1995 bertujuan mengembangkan sistem ISP dengan *wireless*. *Mikrotik* saat ini telah mendukung sistem ISP dengan *wireless* untuk jalur data internet di banyak negara, antara lain Iraq, Kosovo, Sri Lanka, Ghana dan banyak negara lainnya. Berbagai pengembangan telah dilakukan hingga saat ini dengan tersedianya perangkat lunak sistem operasi *router* versi 2 yang menjamin kestabilan, kontrol dan fleksibilitas pada berbagai media antar muka dan sistem *routing* dengan menggunakan komputer standart sebagai *hardware*. Perangkat lunak ini mendukung berbagai aplikasi ISP, mulai dari RADIUS modem *pool*, hingga sirkuit *backbone* dengan DS3. *Mikrotik* berlokasi di Riga, ibukota Latvia, dengan 50 orang karyawan. *Mikrotik* juga menjalankan sebuah ISP kecil, sebagai media percobaan untuk pengembangan *Router*OS *software*.

Gambar 6. *Mikrotik*
(Sumber: *Mikrotik*.com)

a. **Kelebihan dan Kekurangan *Mikrotik***

Gunawan, Simorangkir, and Ghiffari (2018:68) Setelah menggunakan *router Mikrotik*, ternyata ada kelebihan dan kekurangan yang harus diketahui pada *router Mikrotik* agar *administrator* dan *user* dapat memanfaatkannya secara maksimal, yaitu:

1) Kelebihan *Mikrotik*

a) *Mikrotik router* memiliki beberapa fitur yang bisa digunakan sebagai pelengkap untuk membangun sebuah jaringan *internet. Firewall, Nat, Routing, Hotspot, Point to Point Tunneling Protocol,* DNS *Server,* DHCP *Server*.

b) *Admin* dapat mengatur *upload/download limit* pada setiap *user*.

c) Dapat memblokir IP *Address* atau *Mac Address* yang dianggap illegal.

d) *User* bisa mendapatkan jumlah *bandwidth* yang merata, sesuai dengan kebutuhannya masing-masing.

e) Dengan aplikasi tambahan seperti *Winbox* yang memiliki tampilan *user friendly* memudahkan *administrator* untuk melakukan *remote access* pada jaringan.

2) Kekurangan *Mikrotik*

a) *Router Mikrotik* belum mampu menangani sebuah jaringan *internet* dengan skala besar, karena sertifikasi yang dikeluarkan *Mikrotik* tidak seperti *Cisco* yang sudah diakui oleh internasional.

b) Dengan memori yang tidak terlalu besar, *router Mikrotik* harus di *reboot* untuk membersihkan *cache* memori, agar tidak mengganggu kinerja *router*.

8. Pengertian *Router*

Samsumar and Hadi (2018:3) *router* adalah perangkat yang melewatkan paket IP dari suatu jaringan ke jaringan yang lain menggunakan metode *addressing* dan protocol tertentu. *Router-router* yang terhubung dalam jaringan tergabung dalam suatu algoritma *routing* untuk menentukan jalur terbaik yang dilalui paket IP (Sofana, 2012). Proses *routing* dilakukan secara *hop by hop*. IP tidak mengetahui seluruh jalur menuju tujuan setiap paket. IP hanya routing menyediakan IP *address* dari *router* berikutnya yang lebih dekat ke *host* tujuan.

Haryanto (2017:31) *router* adalah perangkat yang akan melewatkan paket IP dari suatu jaringan ke jaringan yang lain, menggunakan metode *addressing* dan *protocol* tertentu untuk melewatkan paket data tersebut. *Router* memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya.

Gambar 7. *Router*
(Sumber: PCMag.com)

Fungsi *router* sebagai berikut Samsumar and Hadi (2018:3):

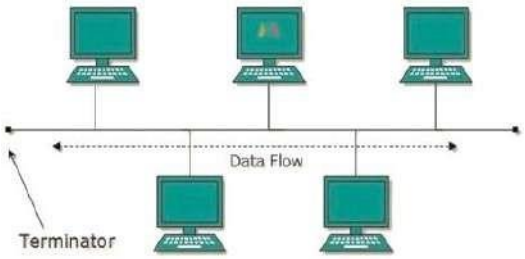
1) Membaca alamat logika/IP *address source* dan tujuan untuk menentukan *routing* dari suatu LAN ke LAN lainnya.
2) Menyimpan *routing table* untuk menentukan rute terbaik antara LAN ke WAN.
3) Perangkat layer ke-3 dalam *Open Systems Interconnection* (OSI) *Layer*.
4) Dapat berupa “box” atau sebuah OS yang menjalankan sebuah *daemon routing*.
5) *Interfaces Ethernet*, Serial, ISDN BRI.

9. Topologi Jaringan

Samsumar & Hadi (2018:2-3) Topologi jaringan komputer secara umum terbagi dalam 6 bentuk sebagai berikut:

a. Topologi *Bus*

Topologi *bus* adalah topologi jaringan yang menggunakan sebuah kabel utama sebagai tulang punggung *(backbone)*. Keuntungan topologi ini adalah hemat kabel, *layou*t kabel sederhana, serta mudah dikembangkan. Kerugiannya adalah deteksi dan isolasi kesalahan sangat kecil, padatnya lalu lintas atau bila salah satu *client* rusak maka jaringan tidak berfungsi dan diperlukan *repeater* untuk menguatkan sinyal untuk jarak jauh.

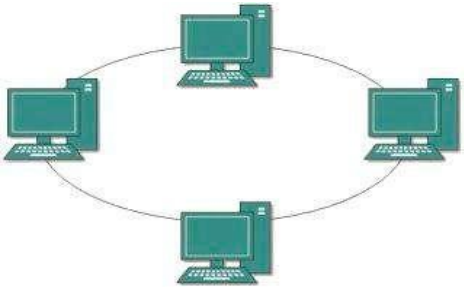


Gambar 8. Topologi *Bus*

(Sumber: Maxmanroe.com)

b. Topologi *Ring*

Topologi *ring* adalah topologi jaringan berupa lingkaran tertutup yang berisi node-node. Semua komputer tersambung membentuk lingkaran. Setiap simpul memiliki tingkat yang sama. Jaringan ini disebut *loop*. Data dikirim ke setiap simpul dan simpul memeriksa alamat informasi yang diterima, apakah untuknya atau tidak. Keuntungan topologi ini adalah pemeliharaan mudah, jarak jangkauan lebih luas daripada topologi *Bus*, laju data *(transfer rate)* tinggi, dapat melayani lalu lintas data yang padat, tidak diperlukan pengendali pusat (*hub/switch*) dan komunikasi antar terminal yang mudah. Kerugiannya adalah penambahan/ pengurangan terminal sangat sulit, tidak kondusif untuk pengiriman suara dan gambar dan kerusakan pada media pengirim akan menghentikan kerja seluruh jaringan.

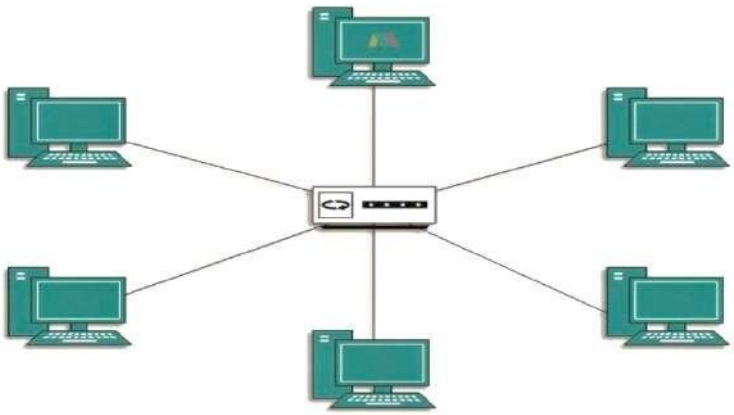


Gambar 9. Topologi *Ring*

(Sumber: Pinterest)

c. Topologi *Star*

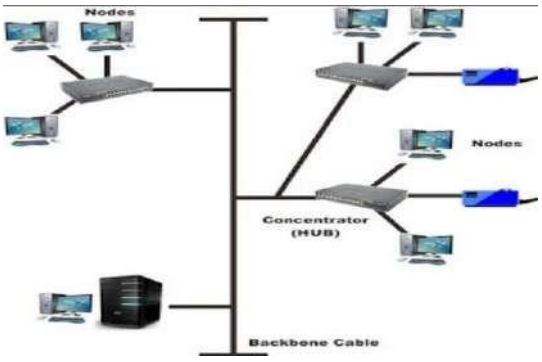
Topologi *Star* adalah topologi jaringan yang menggunakan *concentrator* (*hub/switch*) untuk mengatur paket data. Topologi ini memiliki kontrol terpusat. Semua *link* harus melewati pusat yang menyalurkan data ke semua simpul (*client*). Simpul pusat disebut stasiun primer (*server*), simpul lain disebut stasiun sekunder *(client server).* Setelah hubungan dimulai oleh *server*, setiap *clien*t server dapat menggunakan jaringan tanpa menunggu perintah *server*. Topologi ini adalah paling *fleksibel*. Pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain. Juga memiliki kemudahan dalam pengelolaan jaringan. Kerugiannya antara lain adalah boros kabel, dan *hub/switch* menjadi suatu elemen yang kritis. Topologi *star* merupakan bentuk topologi jaringan yang berupa konvergensi dari node tengah ke setiap node atau pengguna. Masing-masing *workstation* di hubungkan secara langsung ke *server* atau *hub/switch* untuk menghubungkan dari komputer satu ke komputer yang lainnya.



Gambar 10. Topologi *Star*
(Sumber: Maxmanroe.com)

d. Topologi *Tree*

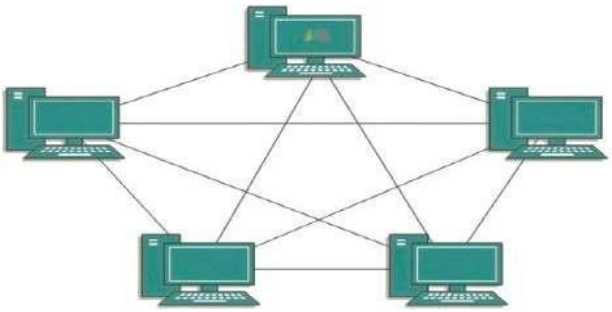
Topologi *Tree* adalah kombinasi topologi *bus* dan topologi *star*. Dalam topologi ini tidak semua node memiliki kedudukan yang sama. Node berkedudukan tinggi menguasai node di bawahnya sehingga node terbawah sangat tergantung pada node diatasnya. Penerapan teknologi ini biasa digunakan pada infrastruktur jaringan LAN antar gedung.



Gambar 11. Topologi *Tree*
(Sumber: Satu Jam)

e. Topologi *Mesh*

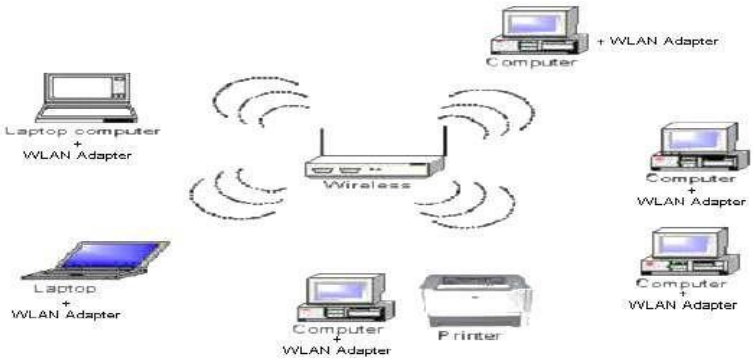
Topologi *mesh* adalah topologi jaringan yang semua komputernya saling terkoneksi satu sama lain. Penerapannya pada jaringan WAN.



Gambar 12. Topologi *Mesh*
(Sumber: Maxmanroe.com)

f. Topologi *Wireless*.

Terdapat 2 jenis topologi yaitu *peer-to-peer* dan *client-server*. Pada topologi *wireless peer-to-peer*, jaringan terhubung pada setiap komputer dalam jaringan dengan lebih mudah dan langsung. Sedangkan pada topologi *wireless clientserver*, harus ada *access point* untuk memungkinkan komputer menerima/mengirim data.



Gambar 13. Topologi *Wireless*
(Sumber: MilkyWay)

10. Perangkat Jaringan Komputer

Menurut Wiharsono Kurniawan (2007), perangkat utama jaringan komputer memiliki peran yang sangat penting dalam suatau jaringan komputer. Apabila salah satu perangkat utama tidak ada, maka suata jaringan tidak akan dapat kita gunakan untuk berkomunikasi antara satu komputer dengan komputer yang lainnya. Memiliki beberapa perangkat keras yaitu:

a. Kartu jaringan

Kartu jaringan merupakan perangkat paling utama yang harus terpasang pada komputer. Setiap komputer dapat kita hubungankan dengan suata jaringan melalaui kartu jaringan. Dengan adanya kartu jaringan, proses tukar-menukar data informasi antara satu komputer dengan komputer yang lainnya dapat terjadi.

Gambar 14. Kartu Jaringan
(Sumber: Distributor Zero Client)

b. Kabel Jaringan

Komputer kita membutuhkan sebuah media transmisi untuk dapat terhubung dan melakukan segala bentuk kegiatan di jaringan. Media transmisi ada beberapa macam bentuk kabel yaitu:

1) Kabel UTP

Kabel UTP sering digunakan pada jaringan untuk menghubungkan komputer. Kabel UTP telah banyak beredar dipasaran, sehingga kita tidak perlu bingung untuk mendapatkannya.

Gambar 15. Kabel UTP
(Sumber: Ayo Konfig!)

2) Kabel STP seperti halnya dengan kabel UTP, penggunaan kabel STP juga digunakan pada jaringan komputer.

Gambar 16. Kabel STP
(Sumber: WordPress.com)

3) Konektor

Konektor adalah peripheral yang kita pasangkan pada ujung kabel UTP. Tujuannya agar kabel dapat kita pasang pada *port* LAN *Card*. Biasanya dalam jaringan komputer konektor yang di pake adalah konektor RJ-45.

Gambar 17. Kabel Konektor
(Sumber: Sory Bro Saya Newbie)

d. Plug Crimper

Plug crimper adalah alat yang digunakan untuk dapat memasangkan ujung-ujung kabel *UTP* dengan konektor RJ-45, maka dieprlukan alat sebuah alat yang dinamakan *Plug Crimp*

Gambar 18. *Plug Crimper*
(Sumber: Home Depot)

e. Hub/switch

Hub merupakan alat yang mempunyai fungsi sebagai tempat untuk menerima *file-file* data dari komputer untuk kemudian meneruskannya ke komputer atau tempat lain pada suata jaringan. Karena menawarkan kinerja transfer dan akses data yang lebih baik, beberapa pemakai lebih senang menggunakan *swtich* dari pada *hub*.

Gambar 19. *Hub/Switch*
(Sumber: Pro.Co.Id)

11. DdoS (*Distributed Denial of Service*)

Menurut Firrar Utdirartatmo (2005:1), *distributed denial of service* (DDoS) merupakan jenis serangan *Denial of Service* (DoS) yang menggunakan banyak *host attacker* untuk menyerang satu buah *host* atau *server* target dalam sebuah jaringan. Dalam sebuah serangan *Distributed Denial of Service* (DDoS) dikategorikan dalam beberapa teknik serangan. *Traffic Flooding* merupakan teknik serangan dengan membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari *client* yang sah tidak dapat masuk ke dalam sistem jaringan.

Request Flooding merupakan teknik serangan dengan membanjiri lalu lintas jaringan dengan banyak *request* terhadap sebuah layanan jaringan yang disediakan oleh sebuah *host* atau server sehingga *request* yang datang dari *client* yang sah tidak dapat dilayani oleh layanan tersebut. Teknik serangan yang terakhir yaitu mengganggu komunikasi antara sebuah *host* atau server dengan *client* yang sah dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan *server.*

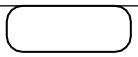
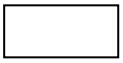
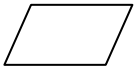
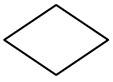
12. Flowchart

Flowchart merupakan urutan-urutan langkah kerja suatu proses yang digambarkan dengan menggunakan simbol-simbol yang disusun secara sistematis (Iswandy, 2015:73).

Flowchart adalah bagan-bagan yang mempunyai arus yang menggambarkan langkah-langkah penyelesaian suatu masalah. *Flowchart* merupakan cara penyajian dari suatu algoritma (Ladjamudin, 2013).

Berdasarkan pengertian yang dikemukakan di atas, dapat disimpulkan bahwa *flowchart* adalah proses atau alur logika suatu aplikasi, sehingga tanpa melihat aplikasi, alur aplikasi dapat dimengerti.

Tabel 1. *Flowchart*

Gambar	Keterangan
	Terminal *Point*: simbol untuk menunjukkan permulaan atau akhir dari suatu proses.
	Simbol Proses: Berfungsi untuk menunjukkan pengolahan yang dilakukan oleh komputer/pc
	Simbol *Input/Output*: berfungsi untuk menyatakan proses input dan *output*
	Simbol Arus: berfungsi untuk menghubungkan antara simbol satu dengan simbol yang lain atau menyatakan jalannya arus dalam suatu proses
	Simbol keputusan (*Decision*): berfungsi untuk memilih proses berdasarkan kondisi yang ada.

(Sumber: Iswandy, 2015:73)

13. Profil Kantor Dinas Pendidikan Kota Palopo

Dinas Pendidikan untuk wilayah Kota Palopo, Sulawesi Selatan merupakan instansi pemerintah yang bertanggung jawab tentang semua hal yang berkaitan dengan pedidikan di wilayahnya. Bertugas melaksanakan urusan pemerintahan Kota Palopo bidang pendidikan berdasarkan asas otonomi dan tugas pembantuan serta melaksanakan tugas-tugas lain berkaitan dengan pendidikan yang diberikan oleh Walikota/Bupati sesuai dengan bidang tugasnya.

Melalui Kantor Dinas Pendidikan ini, pemerintah daerah bidang pendidikan melakukan tugasnya pada wilayah kerjannya. Tugas tersebut mencakup pembantuan urusan pedudukan, pengawasan, penyusunan program pendidikan daerahnya, menyusun strategi, perumusan kebijakan pendidikan hingga

memberikan layanan umum dalam hal pendidikan. Dinas pendidikan ini juga menjadi Pembina dan pemberi izin sekolah dari taman kanak-kanak, sekolah dasar, sekolah menengah pertama, sekolah menengah atas hingga lembaga bimbel.

Adapun Visi Kantor Dinas Pendidikan Kota Palopo yaitu "Menjadikan Kota Palopo sebagai Kota pendidikan yang berkualitas dan berwawasan Agama, Budaya dan Lingkungan yang terkemuka di Indonesia. Sedangkan Misi Kantor Dinas Pedidikan Kota Palopo yaitu mengucapkan perluasan kesempatan memperoleh pendidikan yang berkualitas bagi seluruh warga masyarakat, memberdayakan lembaga pendidikan sebagai pusat pengembangan sumber daya manusia, menyelanggarakan pembelajaran yang berkualitas pada semua jenjang dan jenis satuan pendidikan serta menyelanggarakan pendidikan berdasarkan prinsip otonomi melalui pendidikan gratis paripurna, meningkatkan kuantitas dan kualitas tenaga kependidikan yang mendukung peningkatan mutuh pendidikan menyelanggarakan pelayanan administrasi umum dan mewujudkan kesetaraan dalam memperoleh layanan pendidikan.

Tabel 2. Stuktur Organisasi Dinas Pendidikan Kota Palopo

No	Nama	Jabatan
1	Syahruddin, S.Pd,. Mm	Kepala Dinas
2	Kartini, Sh	Sekretaris
3	Rusnadi, Se	Sub Bagian Umum Pegawaian
4	Furqan Jufri, S.Si	Sub Bagian Perencanaan Dan Keuangan
5	Ishak Idris, S.Sos	Bidang Pendidikan Anak Usia Dini
6	Suyuti Zakir, Ss	Seksi Pembinaan Pendidikan Anak Usia Dini
7	Jufri Pamin, Sh	Seksi Pembinaan Pendidikan
8	Widiastuty, St	Seksi Pembinaan Llembaga Kursus Dan Pelatihan
9	Mahyuddin, S.Kom	Seksi Pembinaan Pendidik Dan Tenaga Kependidikan Sd
10	Yakub Wiratmaja, S.Pd	Seksi Pembinaan Peserta Didik Dan Pembangunan Karakter Sd
11	Mahfullah Dachri, Se	Seksi Pembinaan Pendidikan Dan Tenaga Kependidikan Smp
12	Muh.Haris, Se	Seksi Pembinaan Kelembagaan Dan Sarana Prasarana Smp
13	Dra.Najazi	Seksi Pembinaan Peserta Didik Dan Pembangunan Karakter Smp

2.2 Hasil Penelitian yang Relevan

Bahan penelitian yang ada dan relevan dengan penelitian ini digunakan untuk membantu dalam mempersiapkan penelitian sebagai acuan dan

pengembangan, penelitian yang relevan sangat membantu dalam penyusunan kerangka berfikir.

1. Menurut Penelitian yang dilakukan oleh Widodo & Aji (2022), Tujuan penelitian ini yaitu mengimplementasikan IDS pada sistem jaringan dan menganalisis catatan (*log*) IDS untuk mengetahui jenis-jenis dan tipe serangan jaringan komputer. *Log* pada IDS akan dianalisis secara mendalam untuk digunakan sebagai upaya meningkatkan keamanan jaringan komputer. Hasil penelitian menunjukkan *Network Forensic Investigation Framework* memudahkan proses investigasi ketika terjadi serangan jaringan. *Network Forensic Investigation Framework* efektif digunakan ketika jaringan komputer memiliki aplikasi pendukung keamanan jaringan seperti IDS atau yang lainnya. IDS efektif mendeteksi adanya aktivitas *network scanning* dan serangan DOS. IDS memberikan *alert* pada administrator karena ada aktivitas yang melanggar *rule* pada IDS.
2. Menurut Penelitian yang dilakukan oleh Riadi, Umar & Nasrullor. (2018), Penelitian ini membahas perbandingan terkait *tool* Forensik yang digunakan untuk proses eksaminasi dan analisa. Pengambilan salinan bukti digital dilakukan dengan metode forensik statik, sedangkan tahapan penelitian dan analisa mengadaptasi dan mengimplementasikan metode forensik dari *National Institute of Justice* (NIJ) untuk mendapatkan bukti digital. *Software* pembeku *drive* seperti *Shadow Defender* terbukti berpengaruh terhadap praktik eksaminasi forensik digital terhadap didapatkannya bukti-bukti digital, dengan kondisi tersebut presentase keberhasilannya merestorasi *file* hanya 28,7% sehingga dapat menjadi hambatan dalam proses forensik digital.
3. Menurut Penelitian yang dilakukan oleh Harianto & Setiarini (2021), dengan judul Rancangan Keamanan Jaringan Dengan Menggunakan Model Proses Forensik. Berdasarkan hasil analisis dan pengamatan dari forensik perangkat IoT berupa dua rumah cerdas yang menjadi sasaran penyerang, menunjukkan bahwa aktifitas sistem disimpan dengan baik pada *platform* FAIoT. Hasil analisis membuktikan bahwa serangan terhadap perangkat IoT

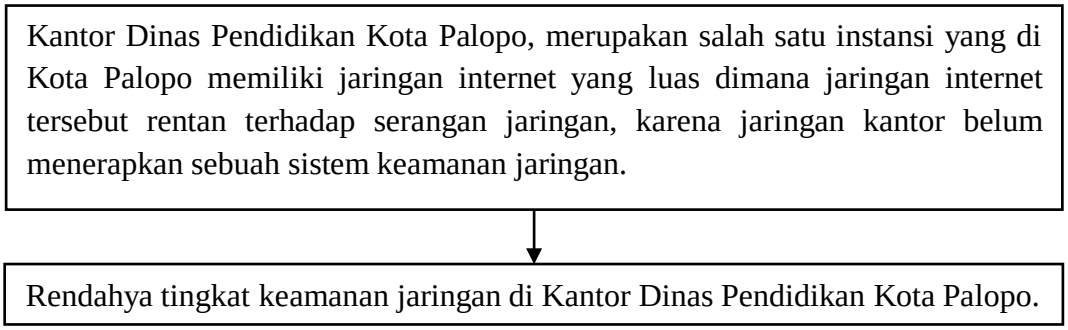
berupa dua rumah cerdas dapat diungkap fakta kasusnya berdasarkan temuan-temuan yang dijadikan barang bukti digital.

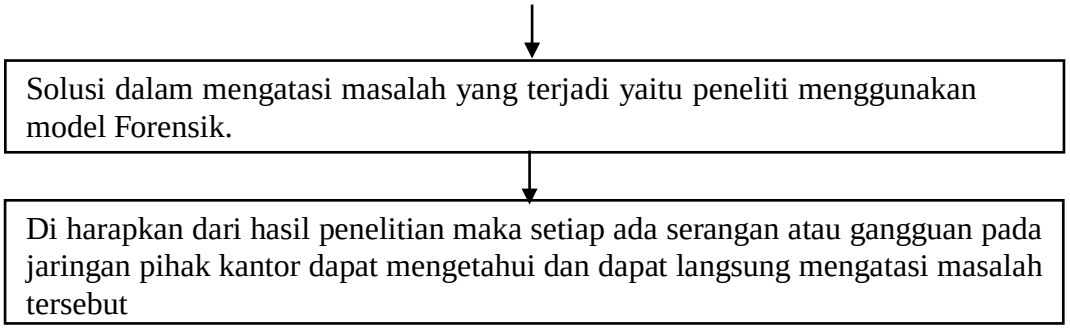
Persamaan penelitian ini dengan ketiga penelitian di atas yaitu pada penelitian pertama sama-sama mengimplementasikan keamanan jaringan, untuk penelitian kedua dan ketiga yaitu mengamankan jaringan komputer dengan model forensik. Sedangkan perbedaan dari ketiga jurnal di atas dengan penelitian yang saya buat yaitu bagaimana cara mengamankan jaringan komputer menggunakan model forensi dengan memfokuskan pada deteksi, pemeriksaan, analisis forensik jaringan, laporan dan tindakan. Pada penelitian pertama hanya memfokuskan keamanan jaringan sedangkan penelitian kedua dan ketiga bagaimana cara menganalisis data dan mendapatkan bukti menggunakan perangkat yang berbeda-beda menggunakan model forensk.

2.3 Kerangka Pikir

Kerangka pikir adalah penjelasan sementara terhadap suatu permasalahan yang menjadi objek yang disusun berdasarkan dari kajian teori dan penelitian yang relevan. Kantor Dinas Pendidikan Kota Palopo merupakan instansi yang terletak di Kota Palopo yang pada saat ini sudah mengalami perkembangan di mana pada proses menggunakan jaringan internet, tetapi pada saat jaringan internet digunakan oleh pegawai sering mengalami gangguan, karena banyak masyarakat luar yang menggunakan wifi, karena Kantor Dinas Pendidikan Kota Palopo belum menerapkan sebuah keamanan jaringan. Adapun sistem yang diusulkan oleh penulis yaitu implementasi keamanan jaringan komputer, diharapkan dengan sistem ini dapat memperbaiki masalah ketika masyarakat dan pegawai yang ada di Kantor Dinas Pendidikan Kota Palopo.

Skema kerangka pikir dalam penelitian ini dapat dilihat pada gambar yang akan disajikan dalam bentuk diagram sebagai berikut:





Gambar 20. Kerangka Pikir