KARYA TULIS ILMIYAH

PENGARUH MALWARE TERHADAP KINERJA JARINGAN KOMPUTER SEBUAH KANTOR (STUDY KASUS KANTOR BUPATI ABDYA)

Di ajukan untuk melengkapi tugas dan memenuhi syarat-syarat

guna memperoleh gelar Ahlimadya Komputer
STMIK U'Budiyah Indonesia

Oleh
Nama : Kudri
Nim : 10123011

PROGRAM STUDI MANAJEMEN INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

(STMIK U'BUDIYAH INDONESIA)

BANDA ACEH

2013

LEMBAR PENGESAHAN SIDANG

PENGARUH MALWARE TERHADAP KINERJA JAINGAN KOMPUTER SEBUAH KANTOR
(STUDY KASUS KANTOR BUPATI ABDYA)

Tugas Akhir/KTI oleh Kudri ini telah dipertahankan didepan dewan penguji padaTanggal : 27 Agustus 2013

Dewan Penguji:

1. Ketua

(Dedi Satria, Msc)

2. Anggota

(T. Khairuman, Msi)

3. Anggota

(Ima Dwitati, MBA

Karya Tulis Ilmiah

Diajukan untuk melengkapi tugas dan memenuhi syarat-syarat
guna memperoleh gelar Ahlimadiya Komputer
STMIK U'Budiyah Indonesia

Oleh
Nama : Kudri
Nim : 10123011

Disetujui,

Penguji I	Penguji II
(T. Khairuman M,si)	**(Ima Dwitati ,MBA)**

Menyetujui,	Disetujui,
Ka. Prodi Manajemen Informatika	Dosen Pembimbing
(Faisal Tifta Zany, M.Sc)	**(Dedi Satria, M,sc)**

Mengetahui,
Ka. STMIK U'Budiyah

(Dr.Amin Haris, MPd)

LEMBAR PERNYATAAN KEASLIAN HASIL

Saya yang bertanda tangan di bawah ini

Nama : Kduri

NIM : 10123011

Progran Studi : Manajemen Informatika

Dengan ini saya menyatakan bahwa Karya Tulis Ilmiah yang saya susun sebagai syarat memperoleh gelar Ahlimadya Komputer merupakan hasil karya tulis saya sendiri. Adapun bagian-bagian tertentu dalam penulisan Tugas Akhir ini yang saya kutip dari hasil karya tulis orang lain dan telah dituliskan sumbernya secara jelas sesuai dengan norma, kaidah dan etika penulisan ilmiah. Saya bersedia menerima sanksi pencabutan gelar akademik yang saya peroleh dan sanksi-sanksi lainnya sesuai dengan peraturan yang berlaku, apabila kemudian hari ditemukan adanya plagiat dalam Karya Tulis Ilmiah ini.

Banda Aceh, 27 Agustus 2013

Yang membuat pernyataan,

(KUDRI)

NIM : 10123011

KATA PENGANTAR

Dengan mengucapkan segala puji bagi kehadirat Allah SWT, yang Maha Pengasih lagi Maha Penyayang, karena dengan rahmat dan hidayah-Nya Proposal Skripsi ini dapat diselesaikan. Shalawat dan salam penulis sanjungkan kepada Nabi Besar Muhammad SAW, beserta para sahabat dan keluarga beliau atas segala perjuangan dan pengorbanan merekalah, kita telah terbebas dari alam kebodohan dan menuju ke alam yang berilmu pengetahuan seperti yang kita rasakan sekarang sampai detik ini.

Alhamdulillah, berkat taufiq dan hidayah-Nya, penulis telah dapat menyelesaikan penulisan Skripsi yang berjudul **"Pengaruh Malware terhadap kinerja Jaringan Komputer Sebuah Kantor (Study kasus Kantor Bupati Aceh Barat Daya".** Penyusunan Skripsi ini disusun untuk memenuhi persyaratan dalam rangka menyelesaikan program studi DIII Manajemen Informatika pada Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK U'Budiyah Indonesia) Banda Aceh. Skripsi ini belumlah mencapai taraf sempurna, karena masih banyak terdapat kekurangan dan kesulitan yang dihadapi dalam proses penyusunan dan penulisan skripsi ini serta keterbatasan ilmu yang penulis miliki. Meskipun pada akhirnya berkat kesabaran dan pertolongan Allah SWT, segala kendala yang menghadang dapat penulis lewati.

Skripsi ini juga tidak akan tersusun bila tidak mendapat dukungan dari berbagai pihak yang memberikan bantuan baik moral maupun spiritual. Oleh karena itu, dalam kesempatan ini penulis mengucapkan terima kasih dan penghargaan yang setinggi-tingginya kepada:

1. Bapak Dedi Zefrizal, ST selaku Ketua Yayasan Pendidikan U'Budiyah Indonesia.
2. Bapak Dr. Amin Haris, M.Pd,selaku Ketua STMIK U'budiyah Indonesia.
3. Bapak Faisal Tiftazany, M.Sc selaku ketua Program Studi Manajemen Informatika.

4. Bapak Dedi Satria, Msc sebagai pembimbing penulis, yang telah meluangkan waktu, tenaga, pikiran serta membimbing penulis dalam menyelesaikan penyusunan Skripsi ini.
5. Dosen-dosen penulis yang telah mentrasfer ilmu kepada penulis selama ini serta staf Akademik STMIK U'Budiyah Indonesia yang telah meluangkan tenaga dan waktunya untuk penulis .
6. Ibunda dan Ayahanda tercinta, yang telah membesarkan dan membimbing penulis baik secara moral maupun secara material, serta do'anya yang tulus sehingga penulis dapat menyelesaikan studi. Tiada yang dapat penulis berikan kecuali rasa hormat, terima kasih, dan cinta yang sedalam dalamnya dan hanya Allah saja kiranya dapat membalasnya dan semoga Ayahanda dan Ibunda senantiasa dalam lindungan Allah SWT. Amiiin…!!!
7. Kepada saudara-saudari penulis Fakhrurrazi dan Asmaul Husna serta Jufrizal terima kasih, Saya sayang kalian.
8. Terima kasih atas masukan dan dorongan kepada sahabat-sahabat penulis, dan Kepada seluruh mahasiswa STMIK U'budiyah Indonesia yang tidak mungkin disebut namanya satu persatu, kakak angkatan`09 terima kasih banyak atas informasi yang kalian berikan, teman-teman seangkatan`10 salam sukses kawan seperjuangan , adik angkatan`11 dan angkatan`12 terima kasih atas segalanya.

Penulis sangat menyadari sepenuhnya, walaupun begitu banyak bantuan dari berbagai pihak, tetapi penulisan proposal ini belumlah sempurna, baik dari segi teknis maupun dari segi penyampaian materi.Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang konstruktif sangat dihargai demi kesempurnaan penyusunan skripsi ini.Akhirnya penulis berharap segala amal baik yang telah dilakukan mendapatkeridhaan Allah SWT, dan dapat memberikan manfaat bagi kita semua.*Amin YaaRabbal 'Alamin…!!!*

Banda Aceh, 27 Agustus 2013

Kudri
10123011

ABSTRAK

Penelitian ini bertujuan untuk mengetahui bagaimanakah kinerja jaringan Komputer yang dipengaruhi oleh Malware yang ada pada Kantor Bupati Aceh Barat Daya,sehingga hasil yang akan diketahui dapat digunakan sebagai bahan acuan dalam pengembangan Kinerja jaringan komputer pada Instansi yang dimaksud, analisa yang digunakan dalam penelitian ini menggunakan Analisa Regresi sederhana, yang dibantu oleh Aplikasi SPSS. Data yang digunakan dalam penelitian ini adalah data primer,Observasi, dengan melakukan wawancara langsung kepada pihak-pihak yang bersangkutan, dan data sekunder yaitu data pelengkap yang sifatnya mendukung keperluan data primer seperti buku-buku, literatur dan sumber-sumber tertulis yang diambil langsung dari objek penelitian. Dari data-data yang diperoleh maka penulis dapat mengumpulkan data yang bisa digunakan dalam pengambilan hasil Analisa,. Dari hasil penelitian penulis dapat menarik kesimpulan bahwa Malware yang menyerang pada Jaringan komputer memiliki pengaruh signifikan terhadap kinerja jaringan komputer. Dimana Malware yang ada dapat memperlambat kinerja jaringan, baik disegi akses sistem maupun akses internet, dan pengiriman Data

Kata Kunci: Malware, Jaringan Komputer,Spss

ABSTRACT

This study aims to determine how the performance of computer networks that are affected by the existing Malware on Southwest Aceh Regency Office , so that the results will be known to be used as a reference in the development of computer network performance at the agency in question , the analysis used in this study using the Analysis simple regression , which is assisted by the SPSS application . The data used in this study is primary data , observations , interviews with the parties directly concerned , and secondary data is data supporting the needs of its complement primary data such as books , literature and writing resources are taken directly from the object of research . From the data obtained , the author can collect data that can be used in decision analysis results , . From the research, the author can draw the conclusion that the Malware that attacks on computer networks has a significant influence on the performance of computer networks . Where existing Malware can slow network performance , both disegi system access and internet access , and delivery of Data

Keywords: Malware, Computer Networking, Spss

DAFTAR ISI

HALAMAN JUDUL

KATA PENGANTAR..... i

ABSTRAK iii

DAFTAR ISI..... iv

DAFTAR GAMBAR..... vi

DAFTAR TABEL iiv

BAB I PENDAHULUAN.....1

Latar Belakang.....1

Rumusan Masalah.....2

Ruang Lingkup.....2

Tujuan Penelitian.....3

Hipotesis.....3

BAB II TINJAUAN PUSTAKA 4

Landasan Teori 4

Pengertian Jaringan Komputer.....4

Tipe Jaringan Komputer.....4

Jenis-Jenis Jaringan Komputer.....6

Pengertian Malware.....8

Jenis Malware.....8

Akibat serangan Malware.....11

BAB III METODOLOGI PENELITIAN 12

Ruang Lingkup Penelitian 12

Tempat dan Waktu Penelitian.....12

Metode Penelitian.....13

Jenis Penelitian.....13

Rancangan Penelitian 13

Metode Pengumpulan Data.....14

Jenis Data.....14

Metode penentuan sampel.....15

Definisi Operasional Variabel penelitian.....16

Variabel terikat (independen).....16

Teknik Analisis Data.....16

BAB IV PEMBAHASAN.....18

Gambaran Umum Instansi .....

4.1.1 struktur Organisasi.....18

Hasil Penelitian.....19

4.2.1 Jumlah sampel berdasarkan spesifikasi Hardisk 19

4.2.3 Jumlah Sampel yang terinfeksi Malware dan tidak terinfeksi.....20

4.2.4 Jumlah Sampel Berdasarkan Kecepatan akses internet.....20

4.3 Analisa 24

4.3.1 Uji Koefisien Regresi (uji t).....30

BAB V PENUTUP.....31

5.1 Kesimpulan.....31

5.2 Saran 31

DAFTAR PUSTAKA.....31

DAFTAR GAMBAR

Gambar 2.1 Local Area Network 7

Gambar 2.2 Metropolitan Area Network 7

Gambar 2.3 Wide Area Network (WAN) 8

Gambar 3.1 Rancangan Penelitian.....14

Gambar 4.1 Struktur Organisasi.....14

DAFTAR TABEL

Tabel 4.1 Jumlah sampel berdasarkan Spesifikasi Hard disk.....16

Tabel 4.2 Sampel yang terinfeksi Malware dan tidak terinfeksi.....16

Tabel 4.3 S Sampel Terinfeksi Dan Tidak Terinfeksi Malware Berdasarkan Kecepatan Akses 17

Tabel 4.4 Jenis Malware dalam Sampel.....20

Tabel 4.5 Tingkat signifikasi (Uji t)) 21

Tabel 4.6 Variable Entered/ Removedb.....21

Tabel 4.7 Model Summary……...21

Tabel 4.8Taraf signifikansi atau linieritas dari regresiANNOVA……...22

Tabel 4.9 Coeficien.....22

Tabel 4.10 Caseview Diagnostic.....28

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam dunia pemerintahan saat ini sudah sangat lazim kita melihat sebuah instansi atau perusahaan menggunakan teknologi komputer yang berbasis web untuk membantu setiap aktifitas dan pengambilan keputusan. Dimana hal tersebut tidak terlepas dari perkembangan teknologi yang semakin meningkat terlebih pada jaringan internet, yang dari tahun ketahun semakin bagus. sehingga penggunanaan teknologi komputer sudah menjadi lumrah dan wajib duugunakan oleh setiap instansi dan perusahaan.

Komputer di masa sekarang sangat berguna untuk memudahkan manusia dalam menyelesaikan berbagai pekerjaan, bahkan setiap hari kita tidak bisa lepas dengan komputer atau sejenisnya, tapi bagaimana jika komputer yang kita gunakan menjadi lambat dalam melakukan berbagai proses, pastinya kita akan sangat terganggu oleh hal tersebut.

Untuk mempermudah dalam menangani setiap masalah yang dihadapi oleh instansi atau organisasi terutama dalam pengiriman data dan juga akses sistem lain nya, banyak perusahaan dan instansi pemerintah menggunakan sistem jaringan komputer yang dihubungkan dengan jaringan internet sehingga dalam pengiriman data lebih cepat dan akurat.

Dalam hal ini seringkali sebuah komputer yang terhubung kejaringan internet yang dijalankan mengalami permasalahan, yang tanpa disadari oleh user akan berakibat buruk bagi keamanan jaringan komputer. sehingga dalam menjalankan sistem dan juga mengakses internet, komputer akan mengalami permasalahan yang sangat serius.

Dimana masalah tersebut berasal dari Malware yang menyerang sistem komputer. Sehingga pengaksesan internet dan sistem komputer yang dijalankan akan mengalami permasalahan dan juga komputer menjadi lambat.

Perlu diketahui bahwa Malware yang saat ini berkembang memiliki kemampuan yang cukup beragam, sebagian besar Malware yang beredar saat ini diantara nya ,Trojan,Worm Spyware, dan Virus yang tanpa disadari akan bekerja setelah di aktifkan oleh pengguna secara sadar maupun tidak sadar (ditempelkan di software2 tertentu yang menarik si pengguna).

Dari segi resiko bahaya Malware memang masih cukup relatif mulai dari hanya sekedar perkenalan malalui popup dan pesan tertulis, melakukan akses keinternet sehingga menambah beban akses, bahkan merusak resource atau sistem yang ada di komputer pengguna, dan yang pastinya virus mengambil sebagian resource memory komputer agar dapat terus bekerja dan bertahan. Salah satu Ciri sebuah komputer terserang Malware adalah lambatnya kinerja komputer tersebut.

Jika dilihat dari besarnya kemungkinan serangan malware terhadap kinerja jaringan komputer, tak tertutup kemungkinan hal ini juga terjadi pada setiap komputer yang digunakan di kantor bupati Aceh Barat Daya.

Dimana badan pemerintahan ini menggunakan sistem komputer yang terhubung dengan jaringan internet untuk membantu penyelesaian setiap urusan pemerintahan yang ditangani.

1.2.Rumusan Masalah

Berdasarakan Latar belakang adapun Rumusan masalah yang bisa diambil dalam penelitian ini antara lain:

1. Bagaimanakah kinerja jaringan komputer yang Terinfeksi Malware pada Kantor Bupati Abdya
2. Bagaimana cara pada Mengatasi Malware yang menyerang sistem jaringan komputer Kantor Bupati Abdya

1.3 Ruang Lingkup

Adapun lingkup masalah yang akan dibahas dalam penelitian ini yaitu, mengetahui bagaimana Malware serta mengetahui dampak yang akan terjadi pada kinerja jaringan komputer perkantoran

1.4 Tujuan Penelitian

1.4.1 Tujuan Umum

Untuk mengetahui bagaimana Pengaruh Malware terhadap Kinerja Jaringan Komputer Pada Kantor Bupati Aceh Barat Daya.

1.4.2 Tujuan Khusus

Melihat sejauh mana Kecepatan Akses jaringan yang dipengaruhi oleh Malware, normal ataukah menurun.

1.5 Hipotesis

Trelease (1960) dalam buku nya “Have to Writre Scientifik And Tekhnical Papers”memberikan definisi hipotesis sebagai “suatu keterangan sementara dari suatu fakta yang diamanati”. Sedangkan Good dan Scates (1954) dalam buku nya “Methods of Research Educational,Psycological,Sociological, Appleton Century-Crofts” menyatakan bahwa “ Hipotesis adalah sebuah taksiran atau referensi yang dirumuskan serta diterima untuk sementarayang dapat menerangkan fakta yang diamati ataupun kondisi yang diamati.(3)

Berdasarkan masalah penelitian, maka dapat dirumuskan hipotesis penelitian ini adalah “Malware berpengaruh terhadap kinerja jaringan komputer perkantoran”.

BAB II
TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 Pengertian Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan hardware/software yang terhubung dengan jaringan. Setiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node.(1)

2.1.2 **Tipe Jaringan Komputer**

Terdapat tiga peran yang dapat dijalankan oleh komputer-komputer di dalam suatu sistem jaringan komputer.Peran pertama adalah menjadi client. Client adalah komputer yang meminta/ menerima sumber daya. Peran kedua adalah menjadi server.

Peran server dalam sistem jaringan komputer yaitu menyimpan dan menyediakan sumber daya untuk diberikan kepada client. Peran ketiga adalah peran dimana salah satu atau semua komputer dalam jaringan menjadi client yang menggunakan sekaligus menyediakan sumber daya yang disebut dengan jaringan peer to peer (P2P) (1)

a. Jaringan Client Server

Client server atau jaringan berbasis server ini didefenisikan dengan kehadiran server di dalam suatu jaringan yang menyediakan mekanisme pengamanan dan pengelolaan jaringan tersebut. File server adalah jantung

dari sistem jaringan ini. Keuntungan dari jaringan client server ini diantaranya:

1. Resource (sumber daya) dan keamanan data terkontrol melalui server.
2. Fleksibel. Maksudnya teknologi baru dengan mudah dapat diintegrasikan ke dalam sistem.
3. Interoperability. Maksudnya semua komponen (client/server/jaringan) saling bekerja sama.
4. Mudah diakses. Maksudnya Server dapat diakses dari jauh dan bisa bekerja di multi platform.

Sedangkan kerugian yang mungkin didapat bila menggunakan sistem jaringan ini adalah selain memerlukan investasi biaya yang cukup mahal juga membutuhkan staf ahli yang mampu mengefisienkan dan merawat jaringan ini.

b. Jaringan Peer To Peer (P2P)

Setiap komputer di dalam jaringan peer to peer mempunyai fungsi yang sama dan dapat berkomunikasi dengan komputer lain yang telah memberikan izin. Secara sederhana dapat dipahami, setiap komputer pada jaringan peer to peer berfungsi sebagi client dan server sekaligus. Jaringan ini biasanya digunakan disebuah kantor kecil dengan jumlah komputer sedikit.Keuntungan menggunakan jaringan peer to peer adalah sebagai berikut:

1. Tidak memerlukan investasi tambahan untuk pembelian hardware dan software bagi server.
2. Tidak memerlukan seorang Network Administrator, serta perawatan mudah dan biaya instalasi yang murah.

Kerugian menggunakan jaringan peer to peer adalah sebagai berikut:

1. Berbagi sumber daya pada suatu komputer di dalam jaringan akan sangat membebani komputer tersebut.

2. Masalah lain adalah kesulitan dalam mengatur file-file. User harus menangani komputernya sendiri jika ditemui masalah
3. Tingkat keamanan jaringan cukup lema

c. Jaringan Hybrid

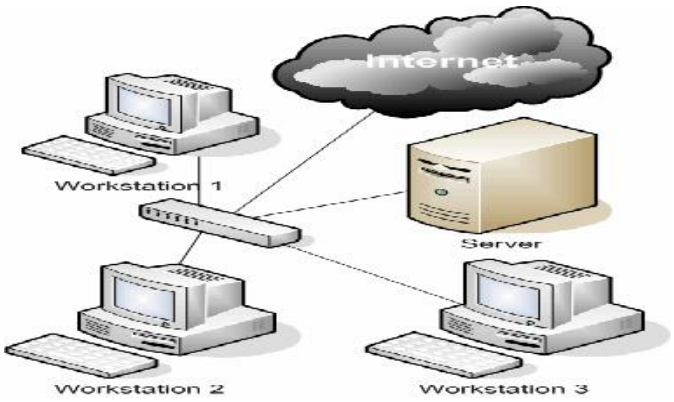
Jaringan hybrid memiliki semua yang terdapat pada dua tipe jaringan sebelumnya. Ini berarti pengguna dalam jaringan dapat mengakses sumber daya yang di share oleh jaringan peer, sedangkan di waktu yang bersamaan juga dapat memanfaatkan sumber daya yang disediakan oleh server.

Keuntungan jaringan hybrid adalah sama dengan keuntungan menggunakan jaringan berbasis server dan berbasis peer to peer. Jaringan hybrid memiliki kekurangan seperti pada jaringan berbasis server

2.2 Jenis-Jenis Jaringan Komputer

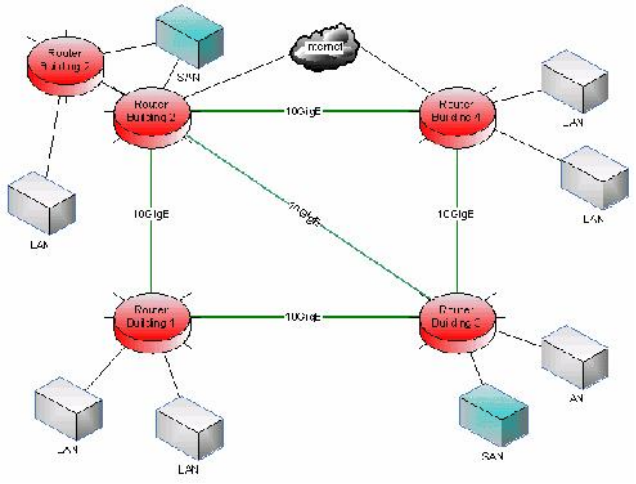
Jaringan komputer dapat dibedakan berdasarkan cakupan geografisnya. Ada empat kategori utama jaringan komputer yaitu :

a. Local Area Network (LAN) Local Area Network (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (resource, misalnya printer) dan saling bertukar



Gambar 2.1Local Area Network

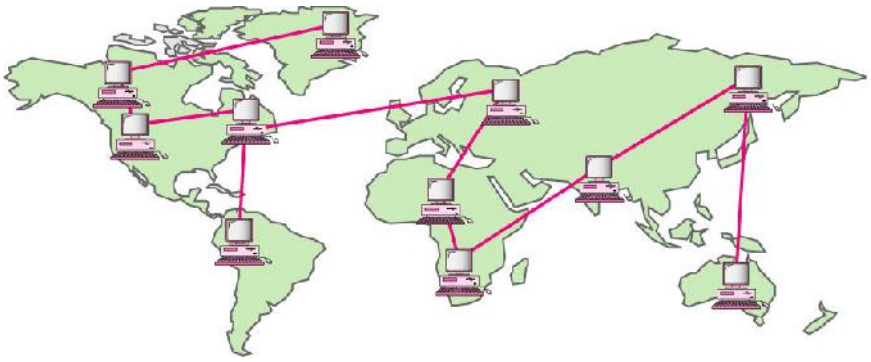
b. Metropolitan Area Network (MAN)Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluanpribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkandapat berhubungan dengan jaringan televisi kabel.



Gambar 2.2 Metropolitan Area Network

c. Wide Area Network (WAN)

Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai..



Gambar 2.3 Wide Area Network (WAN)

d. Global Area Network (GAN)

Global Area Network (GAN) merupakan suatu jaringan yang menghubungkan negara-negara diseluruh dunia. Kecepatan GAN bervariasai mulai dari 1.5Mbps sampai dengan 100Gbps dan cakupannya meliputi ribuan kilometer [(1)]

2.3 Malware

Malware merupakan kependekan dari Malicious Software yang adalah perangkat lunak yang dirancang untuk menyusup ke sistem komputer tanpa persetujuan pemilik atau program komputer yang di rancang untuk tujuan jahat. Malware sendiri terdiri dari berbagai jenis seperti virus, worm, trojan, spyware, dan backdoor..[(3)]

2.3.1 Jenis Malware

1. Virus Komputer

Virus Komputer Merupakan jenis malware yang menyerang file eksekusi (.exe) yang akan menyerang dan menggandakan diri ketika file exe yang terinfeksi di jalankan. Malware jenis ini menyebar melalui interaksi langsung pengguna yang tanpa sadar menjalankan atau memindahkan file yang terinsfeksi virus melalui cd, flashdisk, transfer jaringan atau internet .

Virus komputer merupakan salah satu jenis malware yang menyerang file dan sering kali menggunakan teknik mengelabui dengan menampilkan icon seperti file dokumen atau pun dengan nama file yang memancing user untuk membuka file virus tersebut.

2. Worm Komputer

Worm (Cacing) komputer merupakan jenis malware yang menyerang dan menyebar melalui jaringan. Perbedaan antara worm dan virus adalah dari segi cara penyebaran dan penyerangan. Seperti dijelaskan sebelumnya virus komputer menyebar melalui interaksi pengguna, menyerang file dan aktif jika dijalankan oleh pengguna.

Sedangkan worm menyerang jaringan komputer dengan memenuhi jaringan dengan paket-paket sampah yang membuat koneksi jaringan terhambat dan tidak seperti virus. Worm mampu menyebarkan diri sendiri melalui jaringan dengan memanfaatkan celah keamanan yang terdapat pada sistem komputer tanpa memerlukan interaksi dari pengguna dan akan terus menyebar membentuk sebuah jaringan komputer yang terserang malware yang dikenal sebagai Botnet.

3. Trojan Horse

Trojan Horse merupakan perangkat lunak yang tampak berjalan sesuai fungsinya namun pada kenyataannya menfasilitasi akses yang tidak berhak ke komputer korban. Contohnya jika anda mendownload sebuah program pemutar musik gratis di internet dan menginstalnya,

program tersebut berjalan dengan semestinya memainkan file-file musik namun secara diam-diam program tersebut memfasilitasi seorang hacker untuk mengambil data dari komputer anda.Selain contoh barusan, Trojan horse seringkali memfasilitasi masuknya malware lain seperti worm, spyware dan adware dan tak jarang disisipkan kedalam program freeware.

4. Spyware

Spyware adalah malware yang di rancang untuk mengumpulkan informasi tentang pengguna tanpa sepengetahuan pengguna. Malware jenis ini biasanya dengan sengaja diinstal oleh seseorang ke komputer korban atau pun oleh pengguna lain di komputer bersama seperti warnet dan kantor.

Salah satu jenis spyware adalah *keylogger* (seperti *Refog keylogger* dan lain-lain), keylogger adalah program yang akan mencatat karakter-karakter yang kita ketikan di keyboard, namun keylogger modern saat ini juga mampu mencatat situs-situs yang di kunjungi, text yang di copy paste, hingga program apa saja yang di jalankan. biasanya keylogger di gunakan orang untuk mencuri password, data kartu kredit dan lain-lain.

Kita juga sering mendengar ada yang ribut karena mengaku facebook-nya kena hack atau pun orang yang dengan bangga-nya mengaku bisa meng-hack facebook padahal sebenarnya mereka hanya menggunakan / korban dari keylogger yang di pasang di tempat umum seperti warnet atau kantor

5. Backdoor

Backdoor merupakan metode yang di gunakan untuk melewati autentifikasi normal (*login)* dan berusaha tidak terdeteksi. Backdoor sendiri sering kali disusupkan melalui trojan dan worm.

6. RootKit

Rootkit adalah perangkat lunak yang memungkinkan akses istimewa (*root/administrator*) secara terus menerus. biasanya hacker akan menginstall rootkit pada komputer program untuk mendapatkan hak akses root/administrator dan sering digunakan untuk membuat program tertentu berjalan tanpa terdeteksi. Rootkit sendiri dapat menyerang dalam berbagai mode yaitu user mode, kernel mode, dan boot mode (*bootkit*).

2.3.2 Akibat Serangan Malware

Adapun akibat yang ditimbulkan malware , akan sangat berbahaya bagi data/file bahkan sistem komputer. Malware mampu menyembunyikan file,bahkan merusak sistem.serta memperlambat kinerja jaringan Komputer.

BAB III

METODOLOGI PENELITIAN

3.1 Ruang Lingkup

Ruang lingkup merupakan hal yang sangat penting untuk menentukan sebelum sampai tahap pembahasan selanjutnya, agar pembahasan suatu masalah dalam penelitian dapat terarah atau fokus terhadap suatu tujuan penelitian. Apabila kita mengkaji lebih dalam maka kita dapat melihat luasnya permasalahan yang ada dalam penelitian ini sehingga dibatasi menggunakan ruang lingkup masalah agar penelitian ini dapat menyajikan hasil yang akurat.

Pada penelitian ini, fokus yang paling mendasar adalah bagaimana Malware mempengaruhi kinerja jaringan komputer serta dampak yang akan berakibat bagi masalah perangkat Komputer pada Kantor Bupati Kabupaten Aceh Barat Daya

3.2 Tempat dan Waktu Penelitian

Tempat penelitian merupakan hal yang mendasari pemilihan, pengolahan, dan penafsiran suatu data dan keterangan yang berkaitan dengan apa yang menjadi tujuan penelitian. Penelitian ini dilaksanakan pada Kantor Bupati Aceh barat Daya yang berlokasi di Blangpidie yang dilaksanakan pada tanggal 10 juli samapai dengan 27 juli 2013.

Pemilihan lokasi dilakukan secara sengaja (purposive) dengan pertimbangan bahwa adanya kesediaan lembaga tersebut untuk memberikan informasi yang diperlukan sesuai dengan penelitian. Sedangkan waktu penelitian akan dilaksanan pada bulan juli 2013 sampai dengan selesai.

3.3 Metode Penelitian

Penelitian ini menggunakan study kasus studi kasus menurut Kumar (1999) adalah suatu pendekatan untuk meneliti fenomena sosial melalui analisis

kasus individual secara lengkap dan teliti, serta memberikan suatu analisis yang intensif dari banyak rincian khusus yang sering terlewatkan oleh metode penelitian lain.

Pollit & Hungler (1999) memaknai studi kasus sebagai metode penelitian yang menggunakan analisis mendalam, yang dilakukan secara lengkap dan teliti terhadap seorang individu, keluarga, kelompok, lembaga, atau unit sosial lain. (3)

3.3.1 Jenis penelitian

Dalam penelitian ini adapun jenis penelitian yang digunakan yaitu jenis penelitian statistik deskreptif, membahas tentang statistik deskreptif yaitu " perhatian utama dalam statistik deskreptif adalah menghadirkan informasi dengan tepat, berguna dan mudah dipahami.

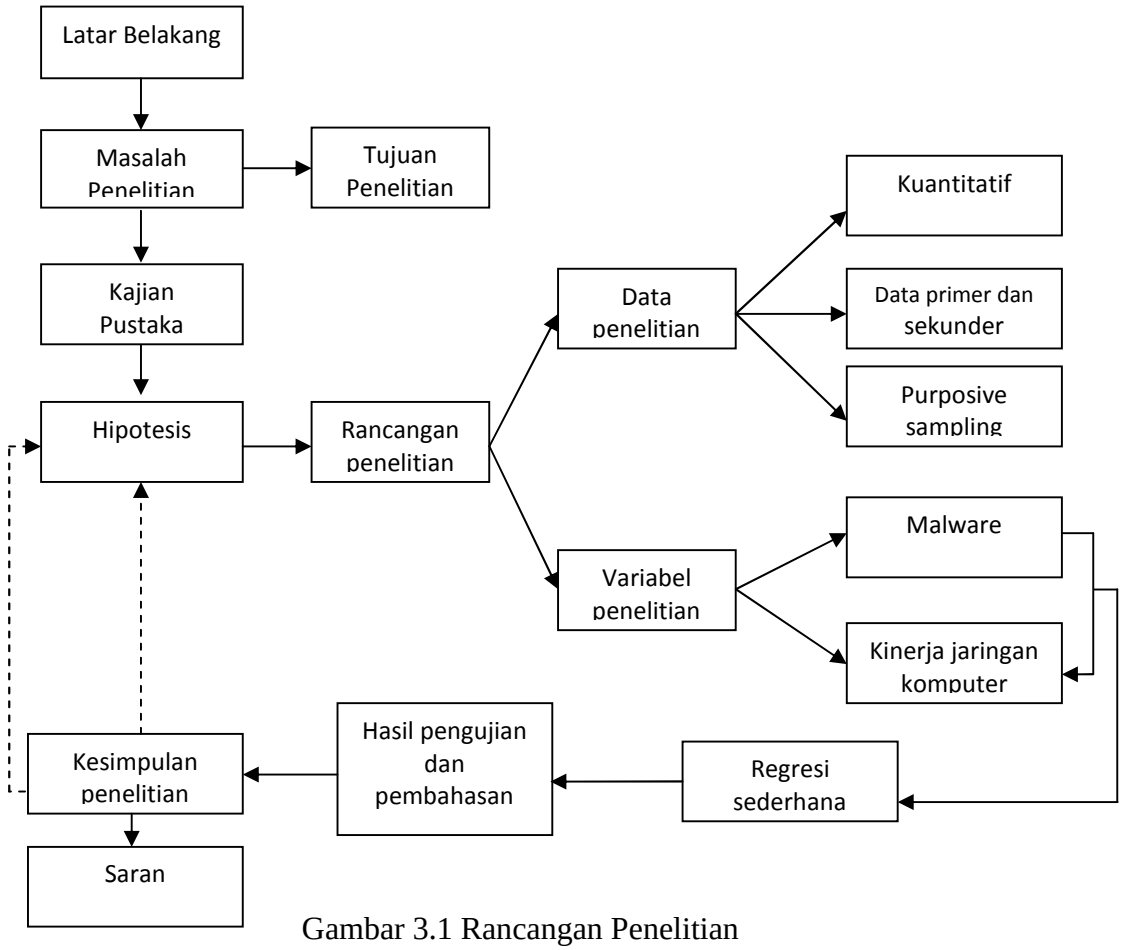
3.4 Rancangan Penelitian

Pada bab sebelumnya telah dijelaskan latar belakang, permasalahan, tujuan, kajian pustaka, dan hipotesis penelitian. Langkah selanjutnya adalah mempersiapkan rancangan penelitian. Rancangan penelitian menjelaskan rencana dan struktur riset yang mengarahkan proses dari hasil penelitian sedapat mungkin menjadi valid, objektif, efisien dan efektif.

Berdasarkan hipotesis penelitian yang diajukan diidentifikasi dua variabel yang digunakan dalam penelitian ini yaitu Malware yang menjadi variabel independen, kinerja jaringan menjadi variabel dependen.

Pengujian terhadap pengaruh Malware terhadap kinerja jaringan komputer menggunakan analisis regresi berganda. Analisis regresi berganda digunakan untuk dapat menunjukan pengaruh variabel independen terhadap variabel dependennya.

Hasil pengujian kemudian dijadikan dasar untuk menarik kesimpulan. Kesimpulan disusun berdasarkan tujuan penelitian (yang ditunjukan dengan garis panah putus-putus). Tahapan-tahapan penelitian di atas (yang ditunjukan dengan panah) disajikan pada Gambar 3.1 berikut ini



Gambar 3.1 Rancangan Penelitian

3.5 Metode Pengumpulan Data

3.5.1 Jenis Data

1. Data primer, merupakan data yang dihimpun sendiri dari responden langsung pada objek penelitian.(3)

   Untuk memperoleh data primer tersebut penulis menggunakan teknik pengumpulan data sebagai berikut :

   a. Pengamatan/ Observasi

      Penulis melakukan pengamatan langsung dengan memantau aktivitas yang dilakukan dalam perusahaan dengan cara mengumpulkan data dengan mengukur pencatatan secara cermat dan sistematis.

2. .Data sekunder, yaitu data pelengkap yang sifatnya mendukung keperluan data primer seperti buku-buku, literatur dan sumber-sumber tertulis yang diambil langsung dari objek penelitian.

3.5.2 Metode penentuan sampel

Penelitian ini menggunakan purpousive sampling. Dimana Sampel dikumpulkan dengan menggunakan kriteria sebagai berikut:

1. Spesifikasi komputer : processor, kapasistas harddisk, memory
2. Kinerja jaringan komputer
3. Jumlah komputer yang terinfeksi virus
4. Kecepatan akses jaringan

Dimana dari parameter diatas dapat dihitung:

1. Jumlah komputer berdasarkan Spesifikasi Hardware
2. Jumlah komputer yang terinfeksi dan tidak terinfeksi Virus
3. Jumlah komputer berdasarkan kecepatan Akses
4. Jumlah komputer berdasarkan performa sistem

Untuk menghitung besarnya sampel yang diperlukan dalam penelitian ini adalah denagn menggunakan rumus yang dikemukakan oleh Yamane sebagai[3] berikut :

$$n = \frac{N}{N\alpha^2 + 1}$$

Dimana

N = Populasi penelitian, diketahui = 100

n = Sampel penelitian

α = taraf signifikansi = 0.05

maka;

$$n = \frac{100}{100(0.05)^2 + 1} = 80$$

Jadi jumlah sampel minimal dalam penelitian ini adalah 80 sampel.

3.6 Definisi Operasional Variabel

3.6.1 Variabel terikat (dependen)

Variabel dependen dalam penelitian ini adalah Malware. Malware adalah perangkat lunak yang dapat mempengaruhi kinerja jaringan komputer.

3.6.2 Variabel bebas (independen)

Variabel independen dalam penelitian ini adalah kinerja jaringan. Kinerja jaringan merupakan kecepatan akses jaringan yang akan di Ukur dengan menggunakan bantuan software *Net meter* dan *Command promt*.

3.7 TeknikAnalisis Data

Teknik analisis data yang digunakan adalah teknik analisis kuantitatif yaitu analisis yang bersifat Objektif dengan berdasarkan angka-angka dalam melakukan penilaian pengaruh Malware terhadap kinerja jaringan komputer `. Alat analisis yang digunakan adalah Regresi sederhana.

Analisis regresi Sederhana Analisis ini untuk mengetahui arah hubungan antara variabel independen dengan variabel dependen apakah positif atau negatif dan untuk memprediksi nilai dari variabel dependen apabila nilai variabel independen mengalami kenaikan atau penurunan.. Data yang digunakan biasanya berskala interval atau rasio.

Dalam penelitian ini, teknik analisis data dilakukan dengan bantuan program SPSS ver 16 for Windows. persamaan regresi ditunjukan dalam persamaan sebagai berikut:

$$(Y' = a + bX)$$

Keterangan:

Y’ = Variabel dependen (Kinerja Jaringan Komputer)

X = Variabel independen

a = Konstanta (nilai Y’ apabila X = 0)

b = Koefisien regresi (nilai peningkatan ataupun penurunan)

BAB IV
PEMBAHASAN

4.1 Sejarah Singkat Instansi

Kabupaten Aceh barat Daya adalah salah satu Kabupaten diprovinsi Aceh ,Indonesia. Kabupaten ini resmi setelah disahkannya Undang-undang Republik Indonesia Nomor 4 tahun 2002.

Aceh Barat Daya sebagai hasil pemekaran dari Kabupaten Aceh Selatan bukanlah merupakan ekses dari reformasi pada atahun 1998 semata. Meskipun perubahan pemerintahan Nasional saat itu mempercepat Pemekaran tersebut Namun wacana itu sendiri sudah berkembang sejak sekitar tahun 1960-an.

Kantor Bupati Aceh Barat Daya adalah sebuah Instansi pemerintah Kabupaten Aceh Barat Daya yang diresmikan sejak tahun 2003. Dimana, Bupati defininit hasil pemilihan Kepala daerah secara langsung yaitu Akmal Ibrahim didampingi Syamsurizal untuk masa bakti 2007-2012. Pasangan ini dilantik oleh gubernur Aceh Irwandi yusuf Untuk menggantikan pejabat Bupati Azwar Umri.

Sebelum Azwar Umri menjadi pejabat Bupati, beliau didahului oleh Teuku Burhanudin sampe.Sedangkan Teuku Burhanudin sampe didahului oleh Nasir hasan Yang sebelum nya menggantikan Baharuddin sebagai Bupati perdana,yang dilantik Gubernur aceh Azwar Abubakar tanggal 18 februari 2006

Kantor Bupati Aceh Barat daya berlokasi Dijalan Bukit Hijau Komplek perkantoran Keude paya Blangpidi, dimana Instansi ini dipimpin oleh Ir, Jufri Hasanuddin dan diwakili Oleh Yusrizal Razali, dimana pasangan ini adalah hasil pemilihan secara langsung masyarakat Aceh Barat daya untuk masa jabatan 2012-2017. Dengan wilayah pimpinan mencakup sembilan kecamatan

4.2 Hasil Penelitian

Penelitian Pengaruh Malware terhadap Kinerja Jaringan Komputer dilaksanakan di Kantor Bupati Aceh Barat Daya yang dimulai dari tanggal 10 sampai dengan 27 juli 2013, sampel pada penelitian ini adalah Komputer yang yang digunakan di kantor Bupati aceh Barat Daya yang sudah disambungkan

dengan Jaringan Komputer.dimana Jumlah sampel yang digunakan dalam penelitian ini adalah 79 sampel.

Peneliian dilakukan melalui Observasi terhadap semua sampel yang akan digunakan untuk mencari nilai pengaruh yang diinginkan sebagai bahan analisa, Adapun Observasi yang dilakukan Untuk mengetahui nilai dari setiap sampel yaitu dengan melakukan *Scanning* terhadap semua sampel yang terinfeksi dan tidak terinfeksi malware untuk mendapatkan jumlah sampel dari kedua nya, serta Mengoptimalkan kinerja Komputer menggunakan *tuneup utility*,.serta menguji kinerja jaringan dengan menggukan *JDauto Speed.*

4.2.1 Jumlah sampel berdasarkan Spesifikasi Hardisk

Data mengenai jumlah sampel berdasarkan Spesifikasi Hardisk dapat dilihat pada tabel 4.1 dibawah ini.

Tabel 4.1 Jumlah sampel berdasarkan Spesifikasi Hard disk

No	Spesifikasi Harddisk	n	Prosentasi
1	Harddisk WDC 500GB	40	50.64%
2	Harddisk Seagate 250 GB	24	30..38 %
3	Harddisk 320 GB	15	18.98 %
Jumlah		79	100 %

Sumber : Olahan Peneliti

Komputer yang menjadi sampel penelitian ini sebagian besar spesifikasi nya 500 GB, dan sebagian lagi mempunyai spesifikasi 250 GB dan 320 GB.

4.2.2 Jumlah Sampel yang terinfeksi Malware dan tidak terinfeksi

Data berdasarkan sampel yang terinfeksi Malware dan tidak terinfeksi dapat dilihat pada tabel 4.2 dibawah ini.

Tabel 4.2 Sampel yang terinfeksi Malware dan tidak terinfeksi

No	Terinfeksi dan tidak terinfeksi	N	Prosentase
1	Terinfeksi	35	43.1%
2	Tidak Terinfeksi	44	56.9%
Jumlah		79	100 %

Sumber : Olahan peneliti

4.2.3 Jumlah Sampel Berdasarkan Kecepatan akses internet

Dari data yang diperoleh dari Observasi terhadap jaringan LAN pada Kantor Bupati Aceh Barat Daya, penulis memperoleh data berupa Jumlah Bandtwith yang disediakan oleh ISP yaitu sebesar 500 MB, dari jumlah tersebut dibagi kepada 135 Host, dengan rata-rata jumlah untuk setiap Host 3.8 MB . Data sampel berdasarkan kecepatan Akses jaringan dengan mengukur kecepatan transfer data disajikan dalam tabel 4.3 berikut ini.

Tabel 4.3 Nilai Sampel yang terinfeksi Malware dan Kecepatan Transmit nya

Sampel	Nilai Malware	Kecepatan akses jaringan (Transmit) /kbps
1	6	1.012
2	6	1.023
3	6	1.034
4	4	1.034
5	4	1.034
6	3	1.093
7	3	1.142
8	3	1.165
9	3	1.167
10	4	1.187
11	3	1.187
12	3	1.188
13	3	1.196
14	3	1.198
15	3	1.198
16	3	1.207
17	4	1.216
18	3	1.235
19	4	1.238
20	6	1.240
21	6	1.241

Sampel	Nilai Malware	Kecepatan akses jaringan (Transmit) /kbps
22	6	1.242
23	4	1.243
24	4	1.245
25	7	1.570
26	5	1.560
27	5	1.667
28	5	1.670
29	2	1.771
30	2	1.775
31	2	1.776
32	2	1.876
33	2	1.889
34	2	1.920
35	3	1.921
36	0	2.322
37	0	2.324
38	0	2.345
39	0	2.421
40	0	2.425
41	0	2.425
42	0	2.441
43	0	2.432
44	0	2.452
45	0	2.489
46	0	2.540
47	0	2.542
48	0	2.620
49	0	2.628
50	0	2.624
51	0	2.628
52	0	2.641
53	0	2.652
54	0	2.653
55	0	2.654

Sampel	Nilai Malware	Kecepatan akses jaringan (Transmit) /kbps
56	0	2.654
57	0	2.659
58	0	2.670
59	0	2.774
60	0	2.782
61	0	2.797
62	0	2.802
63	0	2.825
64	0	2.827
65	0	2.829
66	0	2.832
67	0	2.834
68	0	2.824
69	0	2.831
70	0	2.842
71	0	2.834
72	0	2.833
73	0	2.834
74	0	2.833
75	0	2.837
76	0	2.837
77	0	2.838
78	0	2.839
79	0	2.839

Sumber: Olahan0Penelit

Ket : Nilai 0 adalah Nilai sampel yang tidak terinfeksi

Dari tabel 4.4 dapat dilihat jumlah sampel dan jumlah malware yang menginfeksi setiap sampel, dari Tabel diatas bisa untuk mengetahui jenis malware apa saja yang menginfeks setiap sampel dapat dilihat pada tabel 4.5 berikut.

Tabel 4.5 Jenis Malware dalam sampel

No Sampel	Jenis Malware Yang Menginfeksi Sampel (Dari Hasil Scan Menggunakan Kaspersky)
1	Trojan.loader,(Trojan) W32/Mytob-GH(Worm),Win32Ramnit (virus), sality,win32adware Multiplug (virus), autorun.ifc.(virus) .Panther
2	W32/Mytob-GH, sality, win32adware Multiplug , autorun.ifc (virus)
3	FakeAV.house (virus), kavo.Dll (Virus) , moonlight.A (worm), VBinjectA1 (virus) sality (virus) merlin.bat (scrip virus)
4	Zhola.c (virus), Winkiller (Trojan), sysWjr, (worm), SxS(Virus)
5	Pasdump(Trojan) sality(virus) autorun.ifc (virus) Ramnit.J (virus)
6	Malioboro (worm) autorun.ifc(virus) wi32adwareMultiplug (
7	Kadal (worm) cetix (worm) GEN.ztng (virus)
8	Bluefantasi.C (worm) Blackstar (worm) Ranmit (virus)
9	Blacklove.sorce (worm) Blankon (Virus) Blackrider (worm)
10	Winkiller (Trojan) sality (virus) sysWJR(worm) autorun (virus)
11	Fakefolder (worm) sality (virus) GEN.asda (virus)
12	JavaSE.chile (virus) Wisn32Ranmit (virus) hotlala (Trojan)
13	Cacingkita (worm) brontok.C6 (worm) BroACT (virus)
14	Camvil (virus) keymgr (worm) agent (virus) Bolgi (Trojan)
15	Brontok.C6 (worm) autorun.ifc (virus) buff (worm)
16	Andi.CV (virus) *sality* (virus) BlackRider (worm)
17	*Antukhin.B* (virus) *Sality* (virus) a*utorun (*virus) *archmime* (Trojan)
18	Alphx (Trojan) antiporno (virus) Bluefantasi (worm) sality (virus)
19	Sality (virus), amvo (trojan) autorun.ifc (virus) BroACT (virus)
20	autorun.ifc (virus), s ality (virus) bath.Scrip (virus) doc.Net (virus) keymgr (virus)
21	D.ware (virus) dropper (virus) easy (Trojan) gameHouse (worm) galaxy (virus)
22	Gen.free (virus), sality (virus) blastcln (worm) brontok.C4 (Trojan) W32.beagle.@om (virus) autorun.ifc (virus)
23	cirexB (virus) autorun.ifc (virus) klez.E (virus) cmdRunner (worm)
24	Coolfase.A (virus),crybot (trojan) odex.A (virus) CiberSastra (virus)
25	Sality (virus) Doclink (virus) Exelface (virus) Explorea(virus) faceebookfreezer (virus) Fspswd(Trojan) Gamecape (virus)

26	autorun.ifc (virus) Wisn32Ranmit (virus) BrontokA-21(Trojan) sality (virus)
27	Winkiller (Trojan) sality (virus) fake media.B2 (virus) autorun.ifc (virus) kavo.Dll (Virus)
28	Flashparay (virus) sality (virus) autorun.ifc (virus) Ramnit.J (virus) SxS(Virus)
29	Virustutor(virus) Fspswd(Trojan)

No Sampel	Jenis Malware Yang Menginfeksi Sampel (Dari Hasil Scan Menggunakan Kaspersky)
30	archmime (Trojan) winkiller(virus)
31	autorun.ifc (virus) sysWJR(worm
32	GEN.ztng (virus) sality (virus)
33	Ramnit.J (virus) Blackrider (worm)
34	fake media.B2 (virus) autorun.ifc (virus)
35	NGR.botA5(virus) crybot (trojan)

Sumber :*Olahan Peneliti*

4.3 Analisis Data

Setelah melakukan analisa menggunakan Aplikasi SPSS V16 for Windows, didapat kan hasil Analisa Sebagai berikut yang ditunjukan dengan tabel:

a. Tabel Variables Entered/ Removed menunjukkan mana yang menjadi variable bebas dan variabel Terikat:

4.5 Tabel Variable Entered/ Removed[b]

Variables Entered/Removed[b]

Model	Variables Entered	Variables Removed	Method
1	Malware[a]	.	Enter

a. All requested variables entered.

b. Dependent Variable: kinerja jaringan

c. Tabel Model *Summary*

Tabel 4.6. Model Summary

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate

1	.951[a]	.904	.903	.233786

a. Predictors: (Constant), malware

b. Dependent Variable: kinerja jaringan

Tabel diatas menampilkan nilai R yang merupakan simbol dari nilai koefisien korelasi. Pada tabel diatas nilai korelasi adalah 90.4. Nilai ini dapat diinterpretasikan bahwa hubungan kedua variabel penelitian ada di kategori lemah. Melalui tabel ini juga diperoleh nilai R Square atau koefisien determinasi (KD) yang menunjukkan seberapa bagus model regresi yang dibentuk oleh interaksi variabel bebas dan variabel terikat. Nilai KD yang diperoleh adalah 94,4 yang dapat ditafsirkan bahwa variabel bebas X1 memiliki pengaruh kontribusi sebesar 90,4% terhadap variabel Y dan 9,6% lainnya dipengaruhi oleh faktor-faktor lain diluar variabel X1

d. Tabel Annova

Tabel 4.6 Taraf signifikansi atau linieritas dari regresi ANNOVA

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	37.566	1	37.566	687.314	.000[a]
	Residual	3.990	73	.055		
	Total	41.556	74			

a. Predictors: (Constant), malware

b. Dependent Variable: kinerja jaringan

Tabel Annova digunakan untuk menentukan taraf signifikansi atau linieritas dari regresi. Kriterianya dapat ditentukan berdasarkan uji F atau uji nilai Signifikansi (Sig.). Cara yang paling mudah dengan uji Sig., dengan ketentuan, jika Nilai Sig. < 0,05, maka model regresi adalah linier, dan berlaku sebaliknya. Berdasarkan tabel ketiga, diperoleh nilai Sig. = 0,140 yang berarti > kriteria signifikan (0,05), dengan demikian model persamaan regresi berdasarkan data penelitian adalah tidak signifikan artinya, model regresi linier tidak memenuhi kriteria linieritas.

e. Tabel Coeficients

Tabel 4.7 Coeficien

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.373	.059		57.311	.000
	malware	-.709	.027	-.951	-26.217	.000

a. Dependent Variable: kinerja jaringan

Tabel keempat menginformasikan model persamaan regresi yang diperoleh dengan koefisien konstanta dan koefisien variabel yang ada di kolom Unstandardized Coefficients B. Berdasarkan tabel ini diperoleh model persamaan regresi : Y =3,373 + -0,79 X1

f. Tabel Caseview Diagnostic

Tabel 4.8 Caseview Diagnostic

Casewise Diagnostics[a]

Case Number	Std. Residual	kinerja jaringan	Predicted Value	Residual
1	1.952	1.012	.24669	.765311
2	.324	1.023	.89608	.126918
3	.352	1.034	.89608	.137918
4	-1.305	1.034	1.54548	-.511475
5	-1.305	1.034	1.54548	-.511475
6	-1.983	1.093	1.87017	-.777172
7	-1.858	1.142	1.87017	-.728172
8	-1.799	1.165	1.87017	-.705172
9	-1.794	1.167	1.87017	-.703172
10	-.915	1.187	1.54548	-.358475
11	-1.740	1.188	1.87017	-.682172
12	-1.720	1.196	1.87017	-.674172
13	-1.715	1.198	1.87017	-.672172
14	-1.715	1.198	1.87017	-.672172

15	-1.692	1.207	1.87017	-.663172
16	-1.669	1.216	1.87017	-.654172
17	-.792	1.235	1.54548	-.310475
18	-1.613	1.238	1.87017	-.632172
19	-.779	1.240	1.54548	-.305475
20	.880	1.241	.89608	.344918
21	.882	1.242	.89608	.345918
22	.885	1.243	.89608	.346918
23	-.767	1.245	1.54548	-.300475
24	.063	1.570	1.54548	.024525
25	2.522	1.560	.57139	.988614
26	1.138	1.667	1.22078	.446221
27	1.146	1.670	1.22078	.449221
28	1.404	1.771	1.22078	.550221
29	-1.071	1.775	2.19487	-.419869
30	-1.069	1.776	2.19487	-.418869
31	-.813	1.876	2.19487	-.318869
32	-.780	1.889	2.19487	-.305869
33	-.701	1.920	2.19487	-.274869
34	.130	1.921	1.87017	.050828
35	-.504	2.322	2.51957	-.197565
36	-.499	2.324	2.51957	-.195565
37	-.445	2.345	2.51957	-.174565
38	-.251	2.421	2.51957	-.098565
39	-.241	2.425	2.51957	-.094565
40	-.241	2.425	2.51957	-.094565
41	-.200	2.441	2.51957	-.078565
42	-.223	2.432	2.51957	-.087565
43	-.172	2.452	2.51957	-.067565
44	-.078	2.489	2.51957	-.030565
45	.052	2.540	2.51957	.020435
46	.057	2.542	2.51957	.022435
47	.256	2.620	2.51957	.100435

48	.277	2.628	2.51957	.108435
49	.266	2.624	2.51957	.104435
50	.277	2.628	2.51957	.108435
51	.310	2.641	2.51957	.121435
52	.338	2.652	2.51957	.132435
53	.340	2.653	2.51957	.133435
54	.343	2.654	2.51957	.134435
55	.343	2.654	2.51957	.134435
56	.356	2.659	2.51957	.139435
57	.384	2.670	2.51957	.150435
58	.649	2.774	2.51957	.254435
59	.670	2.782	2.51957	.262435
60	.708	2.797	2.51957	.277435
61	.721	2.802	2.51957	.282435
62	.779	2.825	2.51957	.305435
63	.784	2.827	2.51957	.307435
64	.789	2.829	2.51957	.309435
65	.797	2.832	2.51957	.312435
66	.802	2.834	2.51957	.314435
67	.777	2.824	2.51957	.304435
68	.795	2.831	2.51957	.311435
69	.823	2.842	2.51957	.322435
70	.802	2.834	2.51957	.314435
71	.800	2.833	2.51957	.313435
72	.802	2.834	2.51957	.314435
73	.800	2.833	2.51957	.313435
74	.810	2.837	2.51957	.317435
75	.810	2.837	2.51957	.317435
76	.812	2.838	2.51957	.318435
77	.815	2.839	2.51957	.319435
78	.815	2.839	2.51957	.319435
79	.815	2.839	2.51957	.319435

a. Dependent Variable: kinerja jaringan

Berdasarkan Hasil analisa tabel diatas diperoleh model persamaan regresi :

$$Y = a + bX$$

$$(Y = 3.373 + -079\ X)$$

Angka-angka ini dapat diartikan sebagai berikut:

- Konstanta sebesar 3.373; artinya jika Malware (X) nilainya adalah 0, maka kinerja jaringan (Y') nilainya Positif yaitu sebesar 3.373
- Koefisien regresi variabel (X) sebesar -079; artinya Infeksi mengalami peningkatan1, maka kinerja jaringan (Y') akan mengalami penurunan sebesar.-079 Koefisien bernilai negatif artinya terjadi pengaruh negatif antara Malware dengan Kinerja jaringan komputer , semakin naik tingkat infeksi Malware maka semakin semakin tinggi penurunan kinerja Jaringan Komputer Nilai Kinerja Jaringan yang diprediksi (Y') dapat dilihat pada tabel Casewise Diagnostics (kolom Predicted Value).

  Sedangkan Residual (*unstandardized residual*) adalah selisih antara Kinerja jaringan dengan Predicted Value, dan Std. Residual (*standardized residual*) adalah nilai residual yang telah terstandarisasi (nilai semakin mendekati 0 maka model regresi semakin baik dalam melakukan prediksi, sebaliknya semakin menjauhi 0 atau lebih dari 1 atau -1 maka semakin tidak baik model regresi dalam melakukan prediksi)

4.3.1 Uji Koefisien Determinasi

Dalam uji linear sederhana, Koefisien determinasi digunakan untuk mengetahui prosentase sumbangan pengaruh serentak variabel-variabel bebas terhadap variabel terikat untuk itu digunakan angka-angka pada tabel model *summary.*
Cara menetukan Koefisien Determinasi dengan melihat kolom R2, hasil dari analisa data SPPS. [9]

Berdasarkan tabel Summary diatas adapun nilai korelasi nya adalah 0,904. Nilai ini dapat diinterpretasikan bahwa hubungan kedua variabel penelitian ada di kategori kuat.

Persamaan untuk Koefisien Determinasi sebagai berikut

$$(KD = R2 \times 100\%\ )$$

Melalui tabel ini juga diperoleh nilai R Square atau koefisien determinasi (KD) yang menunjukkan seberapa bagus model regresi yang dibentuk oleh interaksi variabel bebas dan variabel terikat. Nilai KD yang diperoleh adalah 90.4% yang dapat ditafsirkan bahwa variabel bebas X memiliki pengaruh kontribusi sebesar 90.4% terhadap variabel Y dan 9.6% lainnya dipengaruhi oleh faktor-faktor lain.

4.3.2 Uji signifikan (UJi F)

Uji F dilakukan untuk menentukan taraf signifikansi atau linieritas dari regresi. Kriterianya yang ditentukan berdasarkan uji F atau uji nilai Signifikansi (Sig.). dengan ketentuan, jika Nilai Sig. < 0,05, maka model regresi adalah linier, dan berlaku sebaliknya. Berdasarkan tabel Annova diperoleh nilai Sig. = 0,000 yang berarti < kriteria signifikan (0,05), dengan demikian model persamaan regresi berdasarkan data penelitian adalah signifikan artinya, model regresi linier memenuhi kriteria linieritas.

4.3.3 Uji Koefisien Regresi (Uji t)

Uji ini digunakan untuk mengetahui apakah variabel independen (X) berpengaruh secara signifikan terhadap variabel dependen (Y). Signifikan berarti pengaruh yang terjadi dapat berlaku untuk populasi (dapat digeneralisasikan)

Dari hasil analisis regresi di atas dapat diketahui nilai t hitung seperti yang diambil dari tabel 4.7 dengan langkah sebagai berikut:

1. Menentukan Hipotesis

   Ho : Ada pengaruh secara signifikan anatara Malware terhadap Kinerja jaringan Komputer

   Ha : Tidak ada pengaruh secara signifikan antara Malware terhadap kinerja Komputer

2. Menentukan tingkat signifikansi

   Tingkat signifikansi menggunakan a = 5% (signifikansi 5% atau 0,05 adalah ukuran standar yang sering digunakan dalam penelitian

3. Menentukan t hitung

   Berdasarkan tabel diperoleh t hitung sebesar(-26.217)

4. Menentukan t tabel

   Tabel distribusi t dicari pada a = 5% : 2 = 2,5% (uji 2 sisi) dengan derajat kebebasan (df) n-k-1 atau 79-2-1 = 76 (n adalah jumlah Sampel dan k adalah jumlah variabel independen). Dengan pengujian 2 sisi (signifikansi = 0,025) hasil diperoleh untuk t tabel sebesar (1,992) ditentukan berdasarkan tabel T (Tingkat signifikan) [8]

5. Kriteria Pengujian

- Ho diterima jika – t tabel < t hitung < t tabel
- Ho ditolak jika – t hitung < - t tabel atau t hitung > t tabel

6. Membandingkan t hitung dengan t tabel

   H0 ditolak karena -t hitung (-26.217) < -t tabel (1,992). Artinya Malware berpengaruh negatif terhadap Kinerja Jaringan Komputer.