

***PRIVATE TUNNEL BERBASIS ENKRIPSI MENGGUNAKAN  
ALGORITMA AES-128 PADA KEAMANAN DATA PRIVATE  
CLOUD STORAGE***



**JURUSAN TEKNIK INFORMATIKA  
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN  
UNIVERSITAS MARITIM RAJA ALI HAJI  
TANJUNGPINANG  
2024**

**PRIVATE TUNNEL BERBASIS ENKRIPSI MENGGUNAKAN  
ALGORITMA AES-128 PADA KEAMANAN DATA PRIVATE  
CLOUD STORAGE**



**Pembimbing I,**

Hendra Kurniawan, S. Kom., M.Sc.Eng., Ph.D.  
NIP. 198404022014041001

**Pembimbing II,**

Muhamad Radzi Rathomi, S. Kom., M.Cs.  
NIP. 198903252019031014

## HALAMAN PENGESAHAN

Judul : *PRIVATE TUNNEL* BERBASIS ENKRIPSI MENGGUNAKAN ALGORITMA *AES-128* PADA KEAMANAN DATA *PRIVATE CLOUD STORAGE*

Nama : Leonardo Tegarsuan

Nim : 2001020019

Jurusan : Teknik Informatika


telah dipertahankan di depan Dewan Penguji dan dinyatakan lulus  
pada tanggal 23 Juli 2024

### *Susunan Tim Pembimbing Dan Penguji*

Jabatan	Nama	Tanda Tangan	Tanggal
Pembimbing I	Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D.		20/07/2024
Pembimbing II	Muhamad Radzi Rathomi, S.Kom., M.Cs		29/7/24
Ketua Penguji	Ferdi Chahyadi, S.Kom., M. Cs		29/07/2024
Anggota Penguji I	Novrizal Fattah Fahmitra, S. Kom., M. Kom		28/07/2024
Anggota Penguji II	Rifaldi Herikson, S. Kom., M. Kom		29/07/2024

Tanjungpinang, 29 Juli 2024  
Universitas Maritim Raja Ali Haji  
Dekan Fakultas Teknik dan Teknologi Kemaritiman



  
**Ir. Sapta Nugraha, S.T., M.Eng**  
**NIP.198904132015041005**



## PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa skripsi saya yang berjudul *PRIVATE TUNNEL* BERBASIS ENKRIPSI MENGGUNAKAN ALGORITMA *AES-128* PADA KEAMANAN DATA *PRIVATE CLOUD STORAGE* adalah benar karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Jika kemudian hari ternyata terbukti pernyataan saya ini tidak benar dan melanggar peraturan yang sah dalam karya tulis dan hak intelektual maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji.

Tanjungpinang, 30 Juni 2024

Yang Menyatakan,

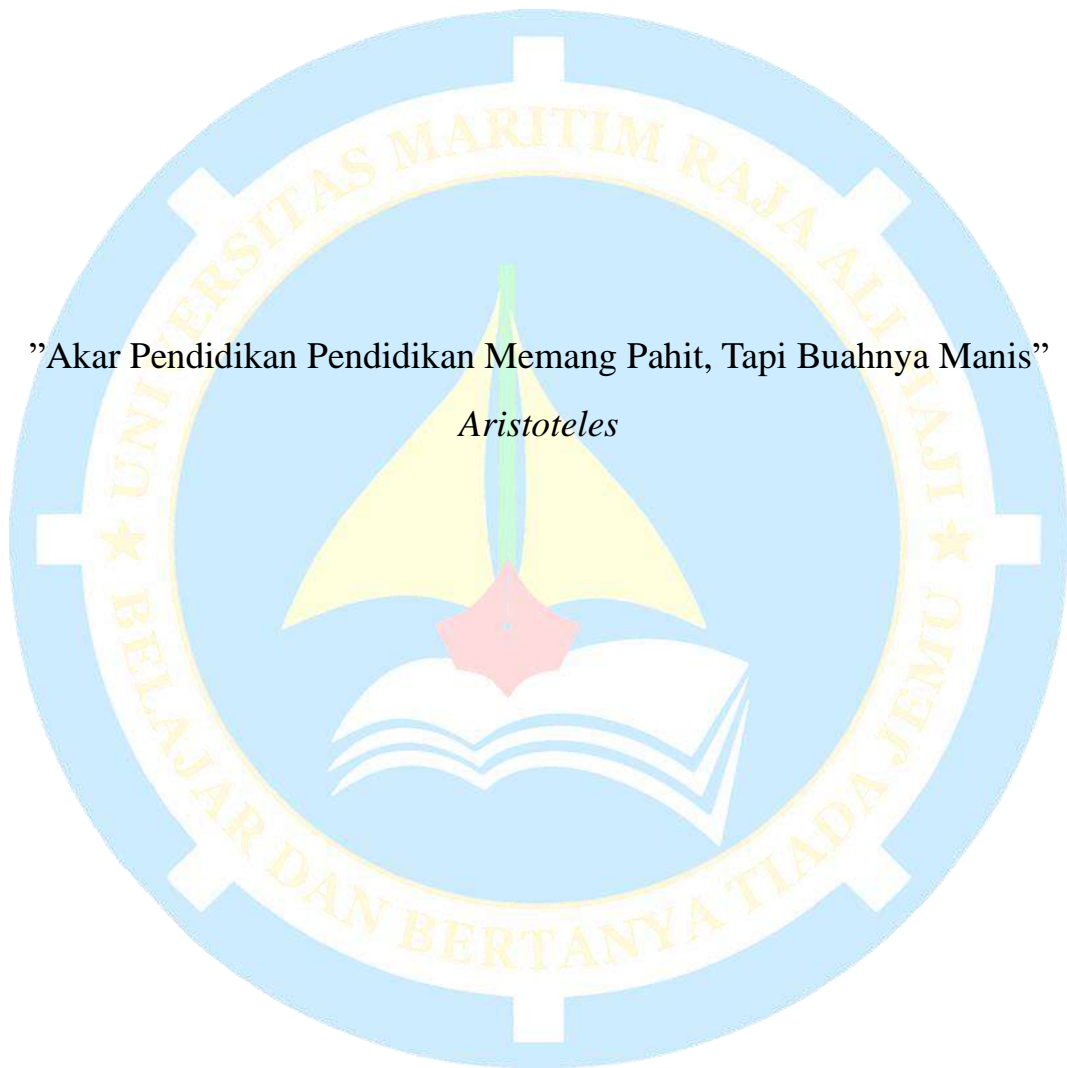


Leonardo Tegarsuan

## HALAMAN MOTO

”Akar Pendidikan Pendidikan Memang Pahit, Tapi Buahnya Manis”

*Aristoteles*



## **HALAMAN PERSEMBAHAN**

**Tugas Akhir ini dipersembahkan untuk:**

### **Tuhan Yang Maha Esa**

Atas segala rahmat dan karunia-Nya yang selalu memberikan kekuatan dan petunjuk hingga tugas akhir ini dapat terselesaikan.

### **Keluarga Tersayang (Ayah, Ibu Abdul, Raka dan Fita)**

Yang selalu mendoakan, mendukung serta memberikan motivasi dan semangat hingga saat ini.

### **Diri Sendiri**

Terima kasih sudah berusaha semaksimal mungkin, selalu bertahan sampai sekarang, dan selalu berusaha untuk tersenyum dan ceria.

Sahabat Tercintaku (Teknik Informatika 2020) Putri Suci Renita, Aznul, Al, Nanda, Fariz, Boyke, Ghora, Ezy, Ilham, Ori, Ervan, Rama, Teti, Irpan, Icad, Miskan, Seto, Rezi, Alwan, Pian, Agnes, Sekar, Arya, Dela, Tiwi, Ejika, Ferya, Jupri, Raju, Tata, Fadli, Fadhly, Mia, Liha, Nifia, Alifa, Raka, Riswan, Siska, Syahri, Yudha, Wan Alfi dan Wan Fariz.

**Program studiku yang sangat ku cintai  
Almamaterku, universitas maritim raja ali haji**

## KATA PENGANTAR

Dengan penuh rasa syukur, penulis mengucapkan puji dan syukur ke hadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi berjudul “*PRIVATE TUNNEL BERBASIS ENKRIPSI MENGGUNAKAN ALGORITMA AES-128 PADA KEAMANAN DATA PRIVATE CLOUD STORAGE*” tepat pada waktunya. Skripsi ini disusun untuk memenuhi syarat memperoleh gelar Sarjana Teknik di Program Studi Teknik Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.

Dalam proses penyelesaian studi dan penulisan skripsi ini, penulis mendapatkan banyak bantuan, bimbingan, dan arahan dari berbagai pihak, baik secara langsung maupun tidak langsung. Oleh karena itu, penulis menyampaikan penghargaan dan terima kasih yang sebesar-besarnya kepada:

1. Ir. Sapta Nugraha, S.T., M.Eng., Dekan Fakultas Teknik dan Teknologi Kemaritiman Universitas Maritim Raja Ali Haji.
2. Bapak Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D., sebagai Pembimbing 1, yang telah memberikan bimbingan terkait penelitian dan penyusunan skripsi.
3. Bapak Muhamad Radzi Rathomi, S.Kom., M.Cs., Ketua Jurusan Teknik Informatika Fakultas Teknik dan Teknologi Kemaritiman Universitas Maritim Raja Ali. Sekaligus pembimbing 2 yang telah bersedia meluangkan waktu untuk memberikan kritik, saran dan arahan kepada penulis.
4. Dan terakhir Ibu Nurul Hayaty, S.T., M.Cs., sebagai pembimbing Akademik, yang telah memberikan bantuan, arahan dan fasilitator ketika saya dalam kesulitan dalam urusan perkuliahan.


Penulis juga menyampaikan terima kasih yang tak terhingga kepada kedua orang tua, M. Nasrun dan Wini Susanti, untuk segala kasih sayang dan dukungannya. Skripsi ini penulis persembahkan untuk mereka. Kesuksesan dan

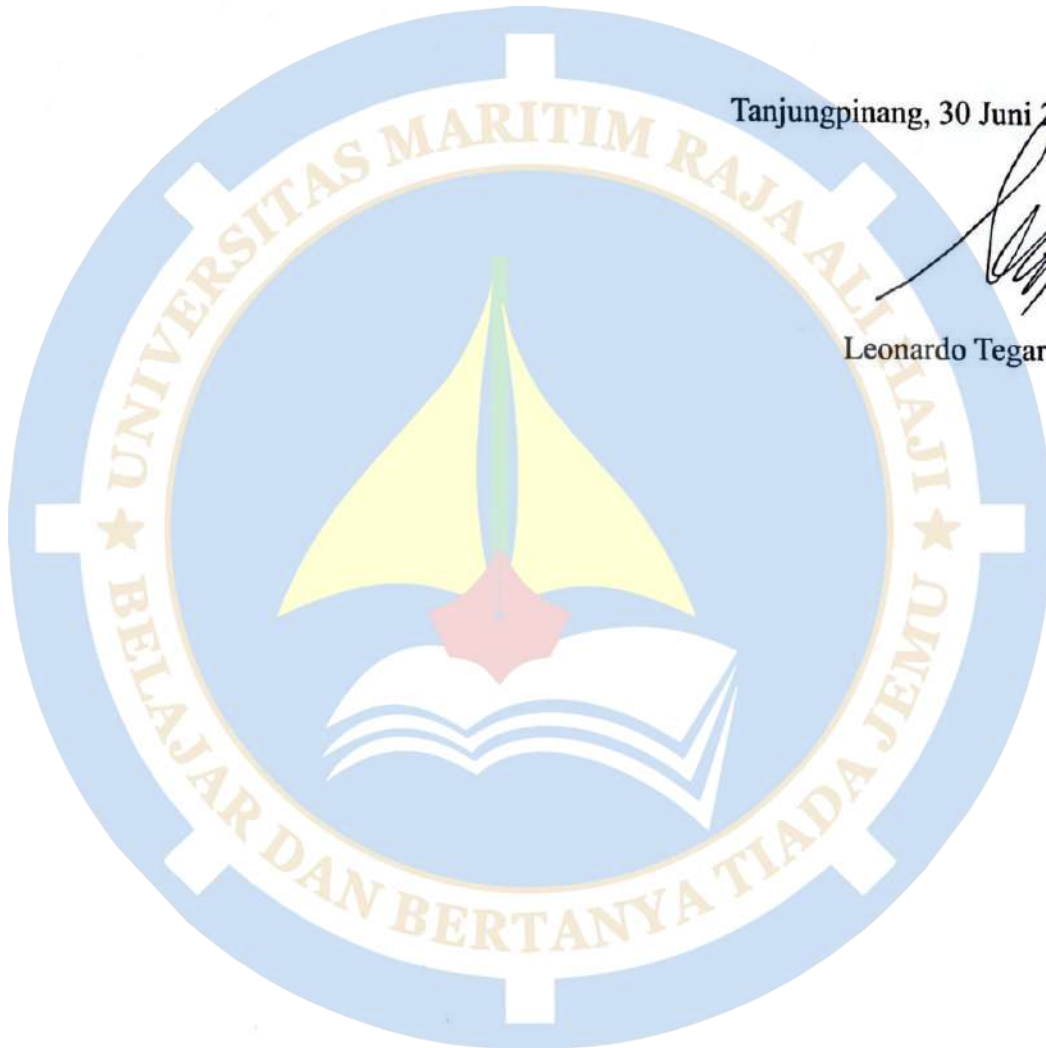


pencapaian penulis adalah berkat doa dan dukungan mereka. Ucapan terima kasih juga disampaikan kepada saudara-saudara penulis Abdul, Raka dan Elfita, tak lupa pula keluarga besar penulis Abdurrahman Family.

Akhir kata, penulis berharap skripsi ini dapat memberikan manfaat bagi pembaca.

Tanjungpinang, 30 Juni 2024

  
Leonardo Tegarsuan





## DAFTAR ISI

HALAMAN JUDUL.....	1
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
PERNYATAAN ORISINALITAS .....	iv
HALAMAN MOTO .....	v
HALAMAN PERSEMBAHAN .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xi
DAFTAR GAMBAR .....	xii
GLOSARIUM.....	xiv
ABSTRAK .....	xv
ABSTRACT.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian .....	5
1.5 Manfaat Penelitian .....	5
BAB II LANDASAN TEORI.....	6
2.1 Tinjauan Pustaka .....	6
2.2 Landasan teori .....	10
2.2.1 <i>Tunneling</i> .....	10
2.2.2 Proses Enkripsi AES-128.....	11
2.2.3 Proses Deskripsi AES-128 .....	14
2.2.4 Model <i>Open Systems Interconnection (OSI) Layer</i> .....	15
2.2.5 <i>File Transfer Protocol (FTP)</i> .....	16
2.2.6 Protokol <i>SSL/TLS</i> dengan <i>OpenSSL</i> .....	16
2.2.7 Wireshark .....	17

BAB III METODE PENELITIAN.....	18
3.1 Waktu dan Tempat Penelitian .....	18
3.2 Tahapan Penelitian .....	18
3.3 Jenis Penelitian.....	18
3.4 Analisis Data .....	19
3.5 Analisis dan Perancangan Sistem .....	19
3.5.1 Perancangan Arsitektur Program .....	20
3.5.2 Perancangan Algoritma Enkripsi AES-128 .....	21
3.5.3 Proses Deskripsi AES-128 Dalam Notasi Matematika.....	31
3.5.4 Perancangan Lingkungan Sistem .....	35
3.6 Implementasi .....	36
3.6.1 program algoritma AES-128.....	36
3.6.2 Persiapan Server.....	43
3.6.3 <i>Generate Certificate Authority</i> dengan <i>OpenSSL</i> .....	46
3.6.3 Program Server.py.....	49
3.6.4 Program Client.py .....	53
BAB IV HASIL DAN PEMBAHASAN .....	54
4.1 Pengujian fungsionalitas program.....	54
4.1.1 Pengujian algoritma <i>AES-128.py</i> .....	54
4.1.2 Pengujian fungsional program server.py.....	55
4.1.3 Pengujian fungsional program client.py .....	62
4.1.4 Pengujian Performa Algoritma .....	64
4.2 Pengujian keamanan jaringan .....	66
4.2.1 Dengan keamanan konektifitas <i>SST/TLS</i> .....	66
4.2.1 Uji hasil enkripsi dan deskripsi data .....	73
BAB V PENUTUP.....	77
5.1 Kesimpulan .....	77
5.2 Saran.....	77
DAFTAR PUSTAKA .....	78

## DAFTAR TABEL

Tabel 1 Instrumentasi Penelitian.....	21
Tabel 2 Percobaan enkripsi dengan 3 skenario.....	55
Tabel 3 Sampel Data Penelitian.....	64



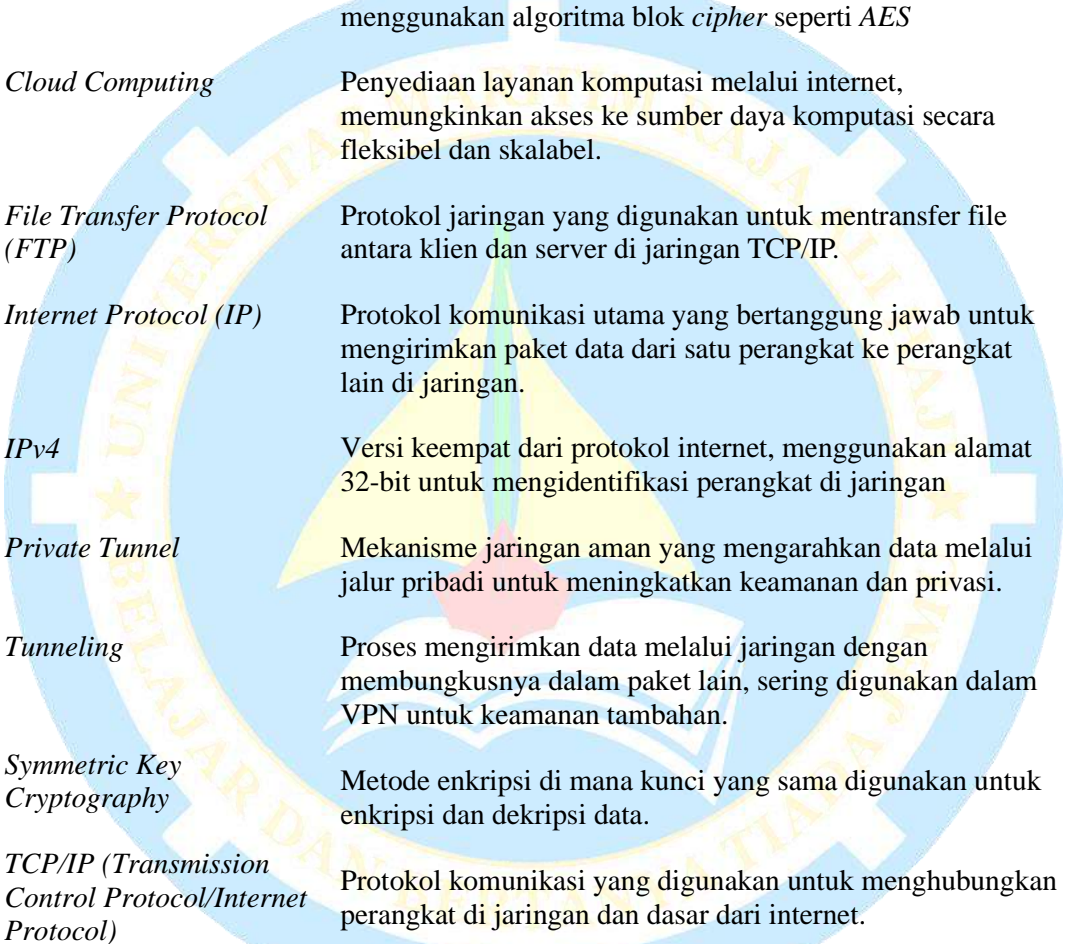
## DAFTAR GAMBAR

Gambar 1 Implementasi Konsep Tunnelling .....	10
Gambar 2 Pola dan cara kerja kunci simetrik .....	11
Gambar 3 Tahapan enkripsi AES.....	12
Gambar 4 Nilai konstanta <i>S-BOX</i> .....	13
Gambar 5 Pencocokan data dengan nilai <i>S-BOX</i> .....	13
Gambar 6 Tahapan <i>shiftRow</i> .....	14
Gambar 7 Tahapan <i>mixColumns</i> .....	14
Gambar 8 Tahapan deskripsi cipher.....	15
Gambar 9 Tahapan penelitian .....	18
Gambar 10 Rancangan pengembangan lingkungan sistem.....	19
Gambar 11 Alur enkripsi pada sistem.....	19
Gambar 12 Alur deskripsi pada sistem .....	20
Gambar 13 Sistem konfigurasi <i>VMWorkstation</i> 16 .....	43
Gambar 14 Proses <i>Installasi Ubuntu Server</i> pada mesin virtual .....	44
Gambar 15 Proses pembaruan sistem operasi <i>Ubuntu Server</i> .....	45
Gambar 16 Proses instalasi <i>SSH-Server</i> .....	45
Gambar 17 Akses <i>remote</i> server menggunakan <i>Putty</i> .....	45
Gambar 18 Membuat kunci private pada <i>openSSL</i> .....	46
Gambar 19 Membuat <i>Certificate Signing Request (CSR)</i> .....	47
Gambar 20 Hasil <i>generate</i> sertifikat pada <i>openSSL</i> .....	48
Gambar 21 Informasi sertifikat <i>self-signed</i> dari <i>openSSL</i> .....	49
Gambar 22 Cara kerja <i>SSL/TLS</i> .....	51
Gambar 23 Alur pengujian program <i>server.py</i> .....	56
Gambar 24 <i>Server.py</i> berjalan.....	56
Gambar 25 Menambahkan <i>user</i> .....	57
Gambar 26 Data user yang telah dienkripsi <i>AES-128</i> .....	57
Gambar 27 Tampilan <i>user interface</i> pada program <i>filezilla</i> .....	57
Gambar 28 <i>Menu site manager</i> pada program <i>filezilla</i> .....	58
Gambar 29 ip, port dan user pada program <i>filezilla</i> .....	58
Gambar 30 <i>log</i> dari program <i>filezilla</i> ketika sukses terkoneksi kedalam server... 58	



Gambar 31 log konektifitas <i>client</i> kedalam server.....	59
Gambar 32 Hasil implementasi <i>TLS/SSL</i> pada <i>server.py</i> .....	59
Gambar 33 lima data uji dengan tipe <i>file</i> yang berbeda.....	60
Gambar 34 blok lima data uji pada direktori <i>client</i> .....	60
Gambar 35 <i>log</i> dan data uji yang telah di upload pada server .....	61
Gambar 36 Hasil <i>store data</i> pada server .....	61
Gambar 37 Alur pengujian <i>client.py</i> .....	62
Gambar 38 Fitur upload pada <i>client.py</i> .....	63
Gambar 39 Fitur <i>download client.py</i> .....	63
Gambar 40 Fitur <i>delete client.py</i> .....	64
Gambar 41 Perbandingan waktu enkripsi .....	65
Gambar 42 Perbandingan waktu deskripsi.....	65
Gambar 43 Tampilan <i>user interface Wireshark</i> .....	66
Gambar 44 <i>User interface server.py</i> .....	67
Gambar 45 Menu autentifikasi <i>login</i> pada <i>client.py</i> .....	68
Gambar 46 <i>User interface client.py</i> .....	69
Gambar 47 Data yang telah <i>terupload</i> dan terenkripsi .....	69
Gambar 48 Hasil analisa <i>traffic capture</i> .....	70
Gambar 49 Aktifitas user dan server terenkripsi dengan algoritma AES .....	71
Gambar 50 Aktifitas client yang terlacak pada keamanan jaringan yang tidak diimplementasikan .....	72
Gambar 51 <i>User interface</i> dari <i>filezilla</i> .....	73
Gambar 52 Percobaan mendapatkan <i>file</i> hasil enkripsi .....	74
Gambar 53 <i>Sample Data</i> uji enkripsi .....	75
Gambar 54 <i>Sample Data</i> hasil enkripsi.....	76
Gambar 55 Kondisi Data menjadi rusak karena data dalam keadaan terenkripsi. 76	

## GLOSARIUM



<i>Advanced Encryption Standard (AES)</i>	Algoritma kriptografi simetris yang menggunakan panjang kunci 128, 192, atau 256 bit untuk mengenkripsi dan mendekripsi data.
<i>Application Layer</i>	Lapisan ke-7 dalam model OSI yang bertanggung jawab untuk komunikasi langsung dengan aplikasi jaringan.
<i>Cipher Block.</i>	Blok data tetap yang dienkripsi sebagai unit tunggal menggunakan algoritma blok <i>cipher</i> seperti <i>AES</i>
<i>Cloud Computing</i>	Penyediaan layanan komputasi melalui internet, memungkinkan akses ke sumber daya komputasi secara fleksibel dan skalabel.
<i>File Transfer Protocol (FTP)</i>	Protokol jaringan yang digunakan untuk mentransfer file antara klien dan server di jaringan TCP/IP.
<i>Internet Protocol (IP)</i>	Protokol komunikasi utama yang bertanggung jawab untuk mengirimkan paket data dari satu perangkat ke perangkat lain di jaringan.
<i>IPv4</i>	Versi keempat dari protokol internet, menggunakan alamat 32-bit untuk mengidentifikasi perangkat di jaringan
<i>Private Tunnel</i>	Mekanisme jaringan aman yang mengarahkan data melalui jalur pribadi untuk meningkatkan keamanan dan privasi.
<i>Tunneling</i>	Proses mengirimkan data melalui jaringan dengan membungkusnya dalam paket lain, sering digunakan dalam VPN untuk keamanan tambahan.
<i>Symmetric Key Cryptography</i>	Metode enkripsi di mana kunci yang sama digunakan untuk enkripsi dan dekripsi data.
<i>TCP/IP (Transmission Control Protocol/Internet Protocol)</i>	Protokol komunikasi yang digunakan untuk menghubungkan perangkat di jaringan dan dasar dari internet.