Analisa Pengaruh Kompresi dan Enkripsi Data Pada Performa Transmisi Data Menggunakan Secure Shell Protocol

G'ray Fridey Gizel Widjaya *1, Billy Susanto Panca #2

Program Studi S1Teknik Informatika,Universitas Kristen Maranatha
Jl. Surya Sumantri No.65, Kota Bandung

[1]Graywidjaya13@gmail.com

[2]Billy.sp@it.maranatha.edu

Abstract — ***In the process of data transmission, there are several things that can affect the speed of data transmission, such as file size and file type. Besides the process of data compression and encryption can also affect the speed of data transmission. Therefore, this study will analyze the effect of data compression and encryption performed on the data transmission process using the secure shell protocol. This research will use several different file types and also have different file sizes. This research will also use some bandwidth limitations in order to find the most efficient use of bandwidth in this data transmission process. The expected final result is that this research can find the effect of data compression and encryption on the performance of data transmission performed and determine which type of transmission is the most efficient for one particular data type.***

Keywords — ***Bandwidth, compression, data transmission, encryption, secure shell protocol***

I. PENDAHULUAN

Di era digital ini, data disimpan dalam berbagai macam format dan disimpan pada perangkat penyimpanan data. Hal ini mengakibatkan semakin banyaknya data yang memiliki ukuran yang besar. Data yang berukuran besar ini akan mempengaruhi lamanya waktu transmisi. Selain itu juga proses transmisi data yang dilakukan belum tentu menjamin keamanan data tersebut. Solusi dari dua persoalan di atas adalah dilakukannya proses kompresi dan enkripsi data pada proses transmisi data yang dilakukan. Proses kompresi dilakukan untuk memperkecil ukuran data yang akan ditransmisikan, hal ini bertujuan untuk mempercepat proses transmisi data tersebut. Sedangkan enkripsi dilakukan agar menjamin keamanan data pada saat dilakukan proses transmisi data. Penelitian ini juga akan dilakukan pada beberapa skenario limitasi *bandwidth* agar dapat menemukan penggunaan bandwidth yang paling efisien.

Penelitian ini akan melakukan proses transmisi data dengan beberapa skenario transmisi data yang berbeda. Hal ini bertujuan agar dapat menemukan skenario transmisi data yang terbaik terhadap suatu tipe data dengan ukuran tertentu.

II. TINJAUAN LITERATUR

A. Transmisi Data

Bandwidth didefinisikan sebagai rentang dalam pita frekuensi atau panjang gelombang. *Bandwidth* juga merupakan jumlah data yang dapat ditransmisikan dalam jumlah waktu yang tetap. Pada perangkat digital, *bandwidth* biasanya dinyatakan dalam *bit per second* (bps) atau *bytes per second* (Bps) [1].

B. Data Rate

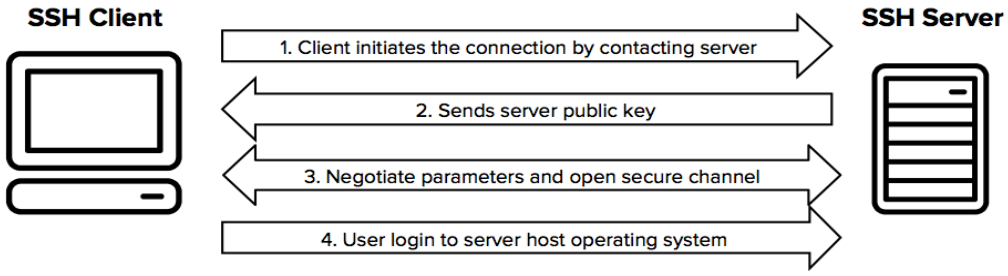
Data Rate adalah istilah untuk menunjukkan kecepatan transmisi, atau jumlah bit per detik yang ditransfer. *Data Rate* dalam telekomunikasi sering dinyatakan dalam *bit per second* (bit/s) Sedangkan dalam komunikasi *Data Rate* sering dinyatakan dalam *byte per second* (B/s) [2].

C. Protokol Transmisi

Protokol pada dasarnya adalah suatu sistem aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data dari dua atau lebih perangkat yang terhubung dalam jaringan tertentu. Sebuah protokol bisa digunakan atau diterapkan pada perangkat keras maupun perangkat lunak. Perlu diperhatikan bahwa protokol yang berbeda dapat memuat jenis-jenis informasi yang berbeda walaupun pada dasarnya sama-sama berjenis informasi digital [3].

D. Secure Shell Protocol

Secure Shell Protocol (SSH) adalah metode untuk mengamankan *remote login* dari satu komputer ke komputer lain. SSH memberikan beberapa opsi alternatif dalam melakukan *authentication* yang kuat, SSH juga melindungi keamanan dan integritas komunikasi dengan sistem enkripsi yang kuat. SSH berfungsi dalam model client-server, yang berarti bahwa koneksi dibuat oleh klien SSH yang terhubung ke server SSH. Klien SSH mendorong proses pengaturan koneksi dan menggunakan *public key cryptography* untuk memverifikasi identitas server SSH. Setelah tahap pengaturan, protokol SSH menggunakan enkripsi simetris yang kuat dan algoritma hashing untuk memastikan privasi dan integritas data yang dipertukarkan antara klien dan server [4].



Gambar 1 Aliran Pengaturan SSH

E. Secure Copy

Secure copy (SCP) adalah protokol transfer file, yang membantu dalam mentransfer file komputer dengan aman dari host lokal ke host jarak jauh. SCP bekerja pada Secure Shell Protocol (SSH). Penggunaan SCP pada penelitian ini bertujuan agar dapat melakukan pengiriman data melalui SSH. Pada SCP juga kita dapat memanfaatkan *command* yang dapat melakukan enkripsi data, kompresi data dan juga limitasi *bandwidth* [4].

F. Packet Switching dan Delays

Packet switching adalah metode transfer data ke jaringan dalam bentuk paket. Untuk mentransfer *file* dengan cepat dan efisien melalui jaringan dan meminimalkan latensi transmisi, data dipecah menjadi potongan-potongan kecil panjang variabel, yang disebut Paket. Di tempat

tujuan, semua bagian kecil ini (paket) harus dipasang kembali, milik *file* yang sama. Paket terdiri dari muatan dan berbagai informasi kontrol [5].

G. Kompresi Data

Kompresi data merupakan proses pengurangan jumlah data yang diperlukan untuk penyimpanan atau transmisi informasi tertentu, biasanya dengan menggunakan teknik pengkodean. Data kompresi dapat berupa *lossless* (*exact*) atau *lossy* (*inexact*). Kompresi *lossless* dapat dibalik untuk menghasilkan data asli, sementara kompresi *lossy* kehilangan detail atau menyebabkan kesalahan kecil saat pembalikan. Kompresi *lossless* diperlukan dalam proses kompresi teks, hal tersebut dikarenakan setiap karakter pada teks tersebut penting, sementara kompresi *lossy* dapat digunakan untuk kompresi gambar atau suara (keterbatasan spektrum frekuensi di telepon menjadi contoh kompresi *lossy*) [6].

H. Gambar

File gambar pada umumnya terbagi ke dalam dua kategori umum yaitu gambar bitmap dan gambar vektor. Setiap kategori tersebut memiliki kegunaan dan keuntungan tersendiri. Pengkategorian ini tidak bisa di bilang sempurna. Karena, format tertentu sebenarnya dapat berisi elemen dari kedua kategori ini.

1. *Gambar Bitmap:* Gambar bitmap terdiri dari sekumpulan titik yang disebut sebagai piksel, di mana setiap piksel tersebut diberi warna secara individu [7].
2. *Gambar Vektor:* Gambar vektor pada dasarnya adalah persamaan matematika raksasa, dan setiap titik, garis, dan bentuk diwakili oleh persamaannya sendiri. Setiap "persamaan" dapat diberi warna, coretan atau ketebalan (di antara gaya lainnya) untuk mengubah bentuk menjadi seni [7].

I. Audio

Dalam tipe data audio, terdapat 3 jenis utama format audio, yaitu tidak terkompresi, kompresi bersifat *lossy* dan kompresi bersifat *lossless.*

1. *Audio Tidak Terkompresi:* Audio yang tidak terkompresi pada dasarnya adalah dari file suara asli. File ini terdiri dari sinyal suara dunia nyata yang telah diubah menjadi *track* audio digital. Jenis format audio ini dapat memberikan kualitas suara yang sangat baik, tetapi ukuran file akan cukup besar dan memerlukan banyak ruang di hard drive [8].
2. *Audio Lossless:* Kompresi lossless dapat menyediakan file audio yang lebih kecil tanpa kehilangan kualitas suaranya. Meskipun kompresi lossless sudah semakin dikenal secara umum, namun sampai saat ini masih belum siap untuk penggunaan skala penuh dikarenakan keterbatasan kapasitas memori sebagian besar perangkat user [8].
3. *Audio Lossy:* Dalam proses kompresi Lossy, terjadi proses yang menghilangkan beberapa data audio asli. Hal ini membuat kualitas audio tersebut akan menjadi sedikit lebih buruk, tetapi ukuran file juga menjadi lebih kecil [8].

J. Video

Dalam tipe data video, terdapat 2 jenis utama format kompresi pada video, yaitu kompresi bersifat *lossy* dan kompresi bersifat *lossless.*

1. *Video Lossy:* Dalam proses kompresi Lossy, terjadi proses yang menghilangkan beberapa data video asli. Hal ini membuat kualitas video tersebut akan menjadi sedikit lebih buruk, tetapi ukuran file juga menjadi lebih kecil [9].
2. *Video Lossless:* Kompresi lossless dapat menyediakan file video yang memiliki salinan piksel demi piksel yang sama dari file asli. Setiap piksel diambil dari sumber dan ditempatkan di file baru persis di mana posisinya di file asli [9].

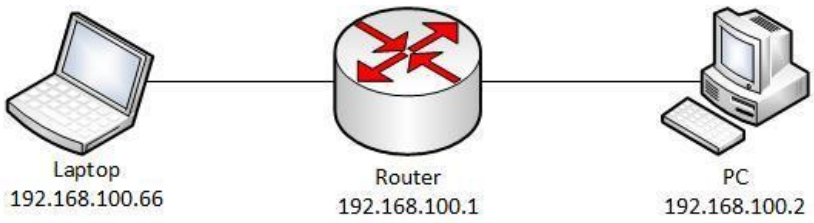
III. METODE PENELITIAN

A. Gambaran Umum

Tujuan dari penelitian ini adalah untuk mendapatkan hasil dari proses transfer data yang dilakukan dengan menggunakan beberapa rancangan transmisi data yang ada, dan menggunakan beberapa tipe data yang berbeda. Dengan adanya hasil dari proses data tersebut, maka nantinya dapat menentukan tipe transmisi data mana yang paling optimal dalam melakukan transfer data suatu tipe data yang ada.

B. Rancangan Topologi

Gambar 2 menunjukan keseluruhan rancangan topologi jaringan yang digunakan dalam penelitian ini.



Gambar 2 Topologi Jaringan

C. Tipe File yang Akan Diuji

Tabel I menunjukan tipe-tipe data apa saja yang akan digunakan pada penelitian ini.

TABEL I

TIPE DATA DALAM PENGUJIAN

Tipe Data	**Nama Format**	**Tipe Kompresi**
Gambar	JPEG	*Lossy*
Gambar	PNG	*Lossless*
Suara	MP3	*Lossy*
Suara	FLAC	*Lossless*
Video	MP4	*Lossy*
Video	AVI	*Lossless*

D. Tipe Cipher

Terdapat 5 cipher yang akan digunakan dalam proses transmisi data penelitian ini, cipher yang digunakan merupakan cipher yang telah tersedia dari *command* SCP. Informasi mengenai cipher tersebut akan dijabarkan pada Tabel II.

TABEL II

TIPE CIPHER DALAM PENGUJIAN

Kode Dalam Pengujian	Cipher
Enkripsi 1	chacha20-poly1305@openssh.com
Enkripsi 2	aes128-ctr
Enkripsi 3	aes192-ctr
Enkripsi 4	aes256-ctr
Enkripsi 5	aes128-gcm@openssh.com

E. Alur Penelitian

Alur penelitian ini akan dimulai dengan membuat jalur transmisi data yang akan dilakukan, dalam penelitian ini akan menggunakan SSH sebagai protokol transmisi jaringan yang akan dibuat. Setelah itu penelitian akan dilanjutkan dengan proses transmisi data dengan menggunakan tipe data serta ukuran yang telah ditentukan sebelumnya. Proses transfer data ini akan menggunakan *command* SCP dalam proses pertukaran data antara komputer klien dan server.

Data yang akan diperoleh dari proses transmisi data sebelumnya akan berupa nilai dari waktu yang dibutuhkan dalam melakukan proses transmisi data tersebut.

Gambar 3 Diagram Alur Penelitian

F. Perangkat Pengujian

Pengujian ini akan menggunakan satu perangkat PC dan satu perangkat laptop. Tabel III akan menunjukan spesifikasi dari setiap perangkat yang digunakan.

TABEL III

SPESIFIKASI PERANGKAT PENGUJIAN

Perangkat	Processor	RAM	Network Card
PC	Intel Core i7 6700K	16.0GB Dual-Channel	Intel(R) Ethernet Connection (2) I219-V
Laptop	AMD Ryzen 7	8.GB Dual-Channel	Realtek USB GbE Family Controller

G. Implementasi SSH

Proses pembuatan jalur transmisi data yang akan digunakan dalam penelitian ini akan menggunakan *Secure Shell Protocol.* Dalam penelitian ini kita akan menginstall OpenSSH *Client* pada PC dan OpenSSH *Server* pada Laptop yang akan berfungsi sebagai *remote side*. Proses pertukaran data antara komputer klien dan server akan menggunakan *command* SCP (*Secure Copy*).

H. Skenario Pengujian

Proses pengujian akan dimulai dengan melakukan proses *download* yang dilakukan oleh komputer *client* kepada komputer *server*. Dalam melakukan proses transmisi data ini terdapat 12 tipe transfer data yang digunakan yang mana di setiap tipe tersebut dilakukan proses kompresi dan enkripsi yang berbeda. Tabel IV akan menjelaskan lebih detail dari setiap tipe transmisi data yang digunakan.

TABEL IV

TIPE TRANSMISI DATA

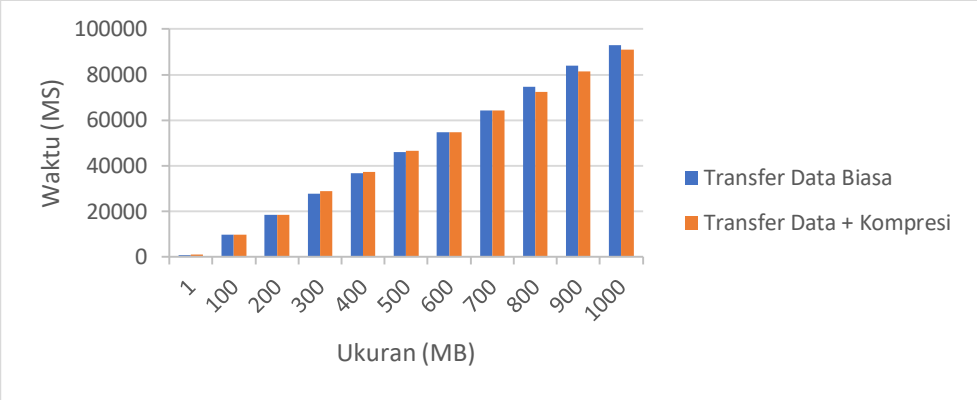
Kode Transmisi Data	Proses Kompresi	Enkripsi
Transfer Data 1	Tidak ada	Tidak ada
Transfer Data 2	Ada	Tidak ada
Transfer Data 3	Ada	chacha20-poly1305@openssh.com
Transfer Data 4	Ada	aes128-ctr
Transfer Data 5	Ada	aes192-ctr
Transfer Data 6	Ada	aes256-ctr
Transfer Data 7	Ada	aes128-gcm@openssh.com
Transfer Data 8	Tidak ada	chacha20-poly1305@openssh.com
Transfer Data 9	Tidak ada	aes128-ctr
Transfer Data 10	Tidak ada	aes192-ctr
Transfer Data 11	Tidak ada	aes256-ctr
Transfer Data 12	Tidak ada	aes128-gcm@openssh.com

Proses perhitungan waktu transmisi total diperoleh dengan menghitung waktu mulai dan waktu berakhir yang akan menggunakan stopwatch class yang dimasukan di dalam script powershell pengujian. Proses pengujian akan dilakukan sebanyak 3 kali untuk setiap tipe *file* dan tipe transmisi data yang dilakukan. Hal ini bertujuan agar mendapatkan hasil yang lebih stabil dengan mengambil rata-rata dari hasil 3 pengujian tersebut.

IV. PENGUJIAN

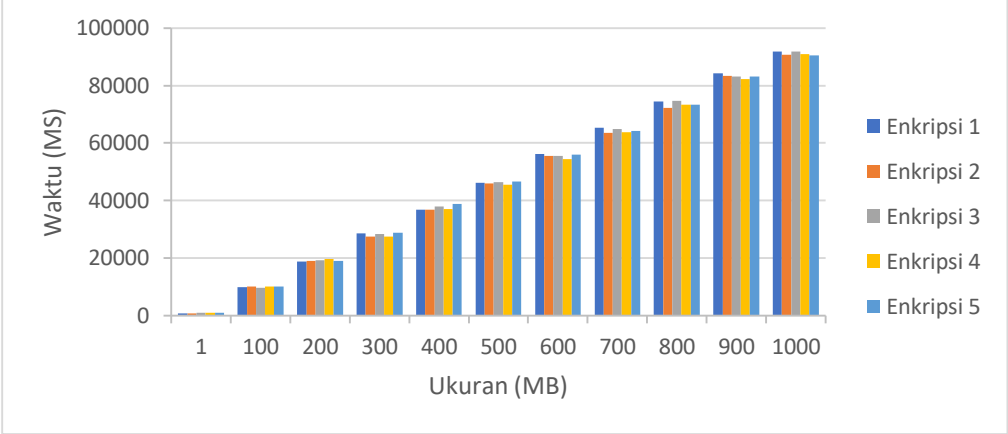
A. Pengujian Tanpa Limitasi Bandwidth

Gambar 4 menunjukan perbandingan antara hasil proses transmisi data yang menggunakan tipe transmisi data yang menggunakan kompresi dan transmisi data yang tidak menggunakan kompresi. Berdasarkan hasil yang ada, maka dapat disimpulkan bahwa penggunaan kompresi tidak efektif jika digunakan pada file yang memiliki ukuran dibawah 800MB.



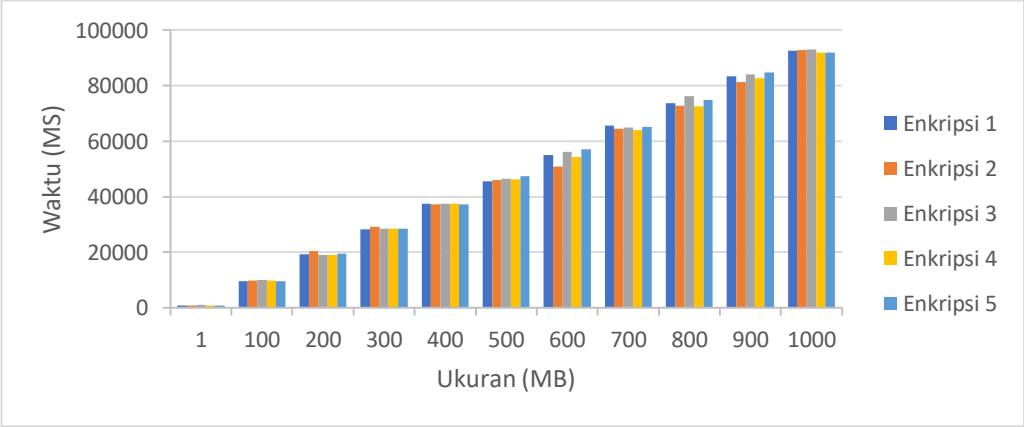
Gambar 4 Perbandingan Transmisi File MP4 yang Menggunakan Kompresi dan Tidak

Gambar 5 menunjukan perbandingan antara hasil proses transmisi data yang menggunakan tipe transmisi data yang menggunakan kompresi dan beberapa tipe enkripsi yang berbeda.



Gambar 5 Perbandingan Transmisi File MP4 yang Menggunakan Kompresi dan Enkripsi

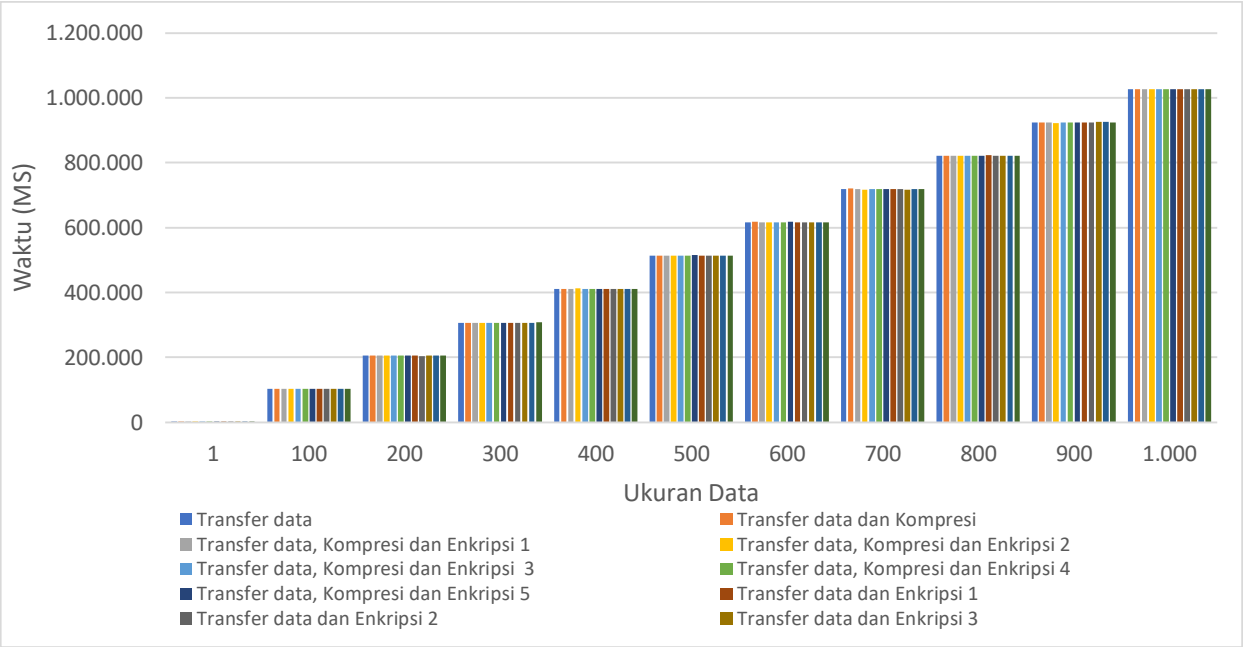
Gambar 6 menunjukan perbandingan antara hasil proses transmisi data yang menggunakan tipe transmisi data yang menggunakan beberapa tipe enkripsi yang berbeda.



Gambar 6 Perbandingan Transmisi File MP4 yang Menggunakan Enkripsi

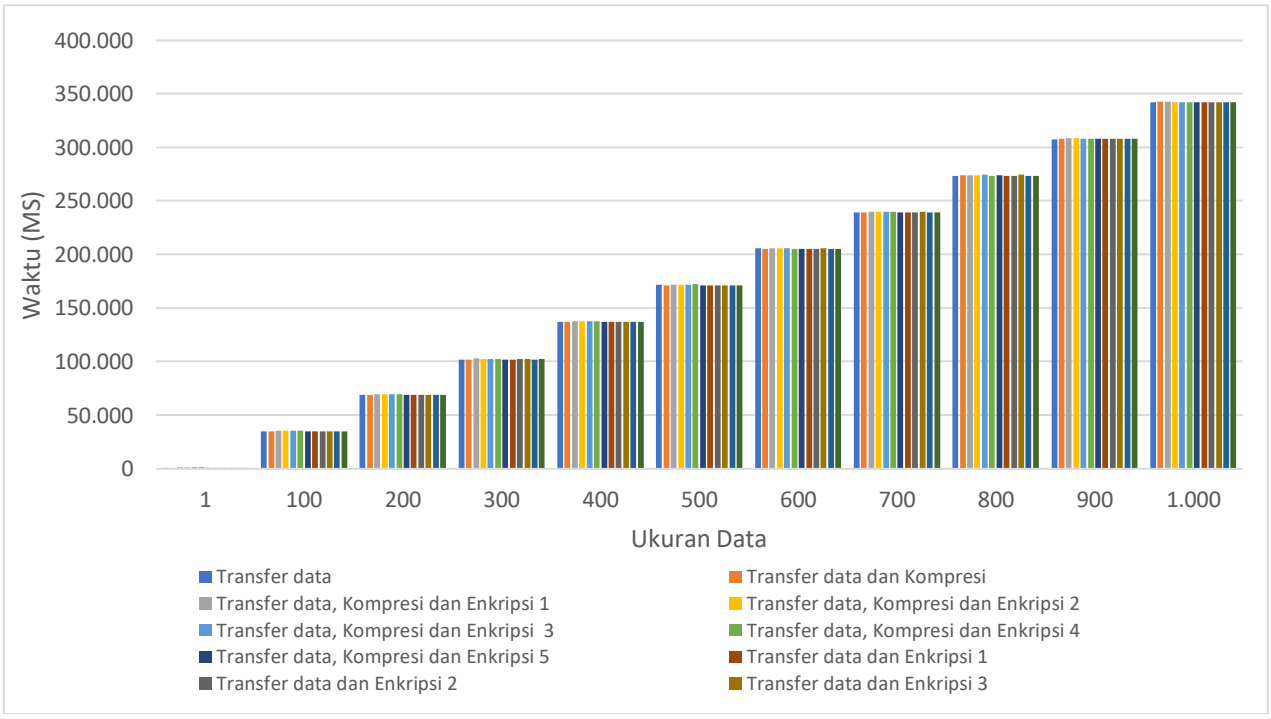
B. Pengujian Dengan Limitasi Bandwidth

Gambar 7 menunjukan perbandingan antara hasil proses transmisi data yang menggunakan limitasi *bandwidth* sebesar 1MB.



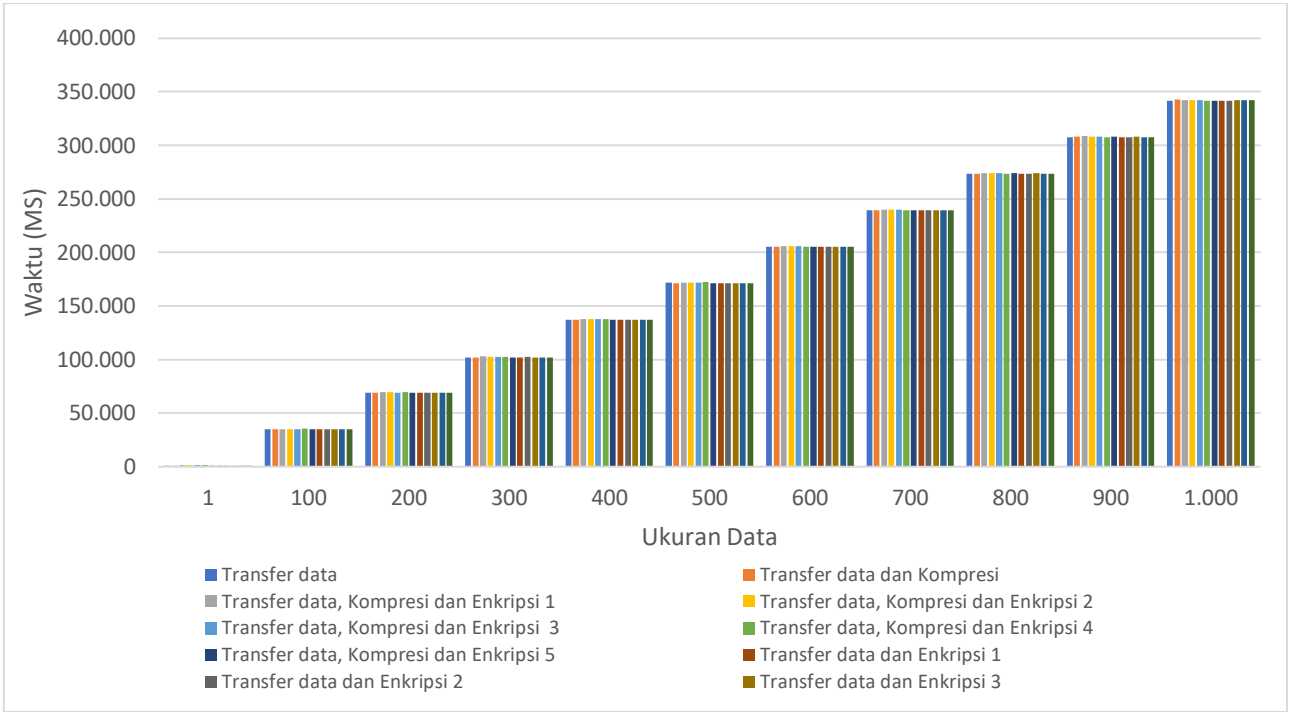
Gambar 7 Perbandingan Limitasi 1MB

Gambar 8 menunjukan perbandingan antara hasil proses transmisi data yang menggunakan limitasi *bandwidth* sebesar 3MB.



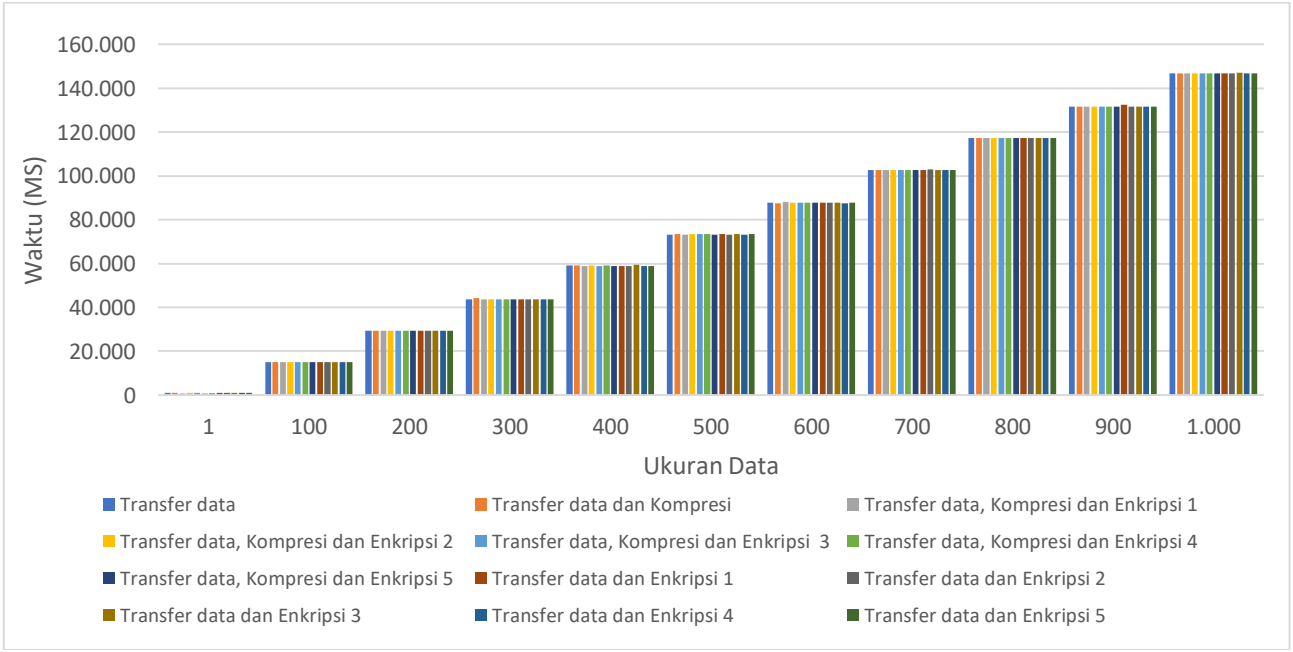
Gambar 8 Perbandingan Limitasi 3MB

Gambar 9 menunjukan perbandingan antara hasil proses transmisi data yang menggunakan limitasi *bandwidth* sebesar 1MB.



Gambar 9 Perbandingan Limitasi 5MB

Gambar 10 menunjukan perbandingan antara hasil proses transmisi data yang menggunakan limitasi *bandwidth* sebesar 1MB.



Gambar 10 Perbandingan Limitasi 7MB

C. Perbandingan Efisiensi Bandwidth

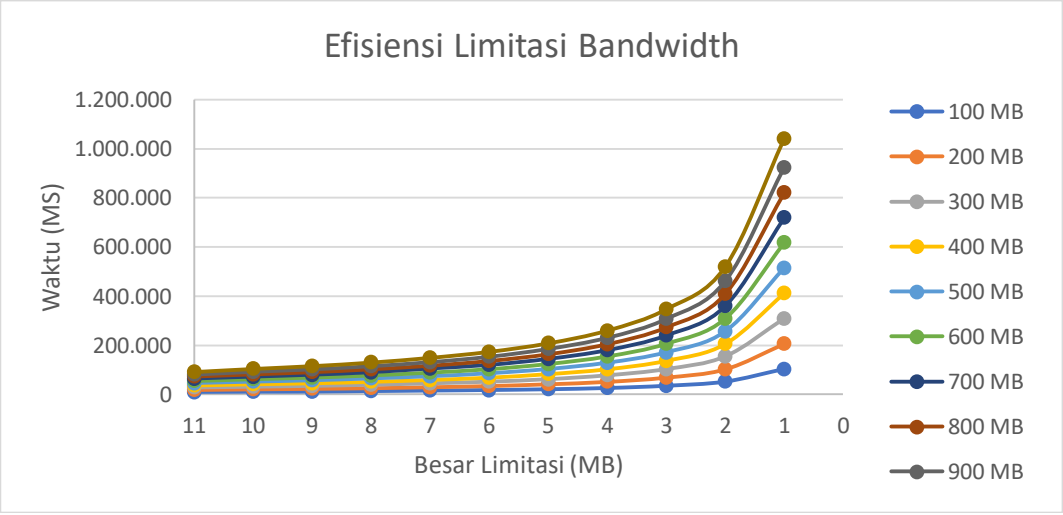
Pada proses perbandingan efisiensi limitasi *bandwidth*, pengujian akan dilakukan menggunakan transmisi transfer data, kompresi dan proses enkripsi tipe 1. Tabel V menunjukan nilai spesifik dari hasil proses transmisi data yang dilakukan.

TABEL V

PERBANDINGAN EFISIENSI LIMITASI BANDWIDTH

Efisiensi Limitasi *Bandwidth*											
Ukuran (MB)	**Waktu (MS)**										
	11	10	9	8	7	6	5	4	3	2	1
100 MB	9,805	10,730	11,096	13,235	15,373	17,592	20,733	25,698	34,762	51,645	102,885
200 MB	18,553	21,220	23,109	25,871	29,807	34,658	41,835	51,634	68,890	102,657	206,212
300 MB	28,164	31,189	34,660	39,096	45,168	51,642	61,933	77,644	103,005	154,767	309,173
400 MB	36,662	41,751	45,759	51,645	59,348	68,679	82,960	102,799	137,066	205,724	411,930
500 MB	46,178	51,695	57,308	64,850	73,757	85,804	103,145	128,768	171,207	256,772	515,119
600 MB	54,690	62,192	68,848	77,469	89,075	102,851	123,976	154,697	206,378	308,837	617,231
700 MB	64,280	72,066	79,840	89,959	105,226	119,822	144,366	179,880	239,831	359,946	719,564
800 MB	73,520	82,476	91,309	103,046	117,666	136,845	164,166	205,243	273,486	409,884	821,621
900 MB	81,292	92,948	102,804	115,624	132,032	153,881	185,691	230,979	307,569	461,802	924,181
1000 MB	91,638	104,191	115,644	130,093	149,266	173,652	208,212	259,954	346,761	519,901	1,040,964

Gambar 11 menunjukan perbandingan hasil transmisi data yang menggunakan limitasi *bandwidth* sebesar 11MB sampai dengan 1MB. Berdasarkan hasil yang didapat proses limitasi *bandwidth* pada besaran 11MB sampai 3MB tidak memiliki dampak yang begitu besar pada kecepatan transmisi data. Akan tetapi ketika kecepatan transmisi data naik drastis ketika proses limitasi *bandwidth* dilakukan pada besaran 2MB dan 1MB. Hal ini menunjukan bahwa besar limitasi *bandwidth* yang paling optimal adalah 3MB.



Gambar 11 Perbandingan Efisiensi Limitasi Bandwidth

V. KESIMPULAN

A. Kesimpulan

Berikut adalah kesimpulan yang didapat dari hasil penelitian dan pengolahan data yang didapat setelah melakukan pengujian transmisi data, pengelompokan data dan analisa data:

1. Hasil pengujian transmisi data dilakukan menggunakan SCP melalui *protocol* SSH, proses kompresi dan enkripsi juga menggunakan *command* yang disediakan oleh SCP. Dari hasil yang ada, ditemukan bahwa proses kompresi dan enkripsi yang dilakukan memberikan pengaruh yang tidak begitu besar terhadap performa transmisi data yang terjadi. Hal ini berdasarkan pada nilai hasil transmisi yang tidak menunjukan kenaikan ataupun penurunan performa yang signifikan terhadap proses transmisi data yang terjadi. Oleh sebab itu, penggunaan kompresi dan enkripsi pada proses transmisi data baik digunakan karena dengan adanya proses enkripsi yang dilakukan dapat menjamin keamanan data yang dikirimkan, terlebih lagi karena proses enkripsi yang dilakukan tidak mempengaruhi performa transmisi data yang terjadi secara signifikan.
2. Tipe data yang digunakan pada proses penelitian ini tidak mempengaruhi performa durasi transmisi.
3. Besar limitasi *bandwidth* yang paling optimal berada pada besaran 3MB. Di bawah itu kecepatan transmisi memiliki pertambahan waktu transmisi data yang sangat signifikan.

B. Saran

Berikut adalah saran yang dapat diberikan untuk mengembangkan hasil dari penelitian dan pengolahan data yang telah didapat:

1. Penelitian selanjutnya sebaiknya menggunakan tipe file dan ukuran file yang lebih banyak agar mendapatkan data pengujian yang lebih lengkap.
2. Penelitian selanjutnya dapat menggunakan tipe-tipe enkripsi lainnya yang belum digunakan pada penelitian ini.

DAFTAR PUSTAKA

[1] B. Saltzberg, "Performance of an Efficient Parallel Data Transmission System," in IEEE Transactions on Communication Technology, vol. 15, no. 6, pp. 805-811, December 1967.
[2] Guok, Chin & Lee, Jason & Berket, Karlo. Improving the bulk data transfer experience. IJIPT. 3. 46-53. 10.1504/IJIPT.2008.019295, 2008.
[3] A. Jungmaier, E. Rescorla, M. Tuexen, Transport Layer Security over Stream Control Transmission Protocol, 2002.
[4] T. Kasas, "Secure Shell Connection — SSH and Secure Copy — SCP," 30 September 2019. [Online]. Available: https://medium.com/q-software/secure-shell-connection-ssh-and-secure-copy-scp-3a9b4ffcf68f. [Diakses 16 Januari 2020].
[5] Robert M. Metcalfe and David R. Boggs. Ethernet: distributed packet switching for local computer networks. vol. 19, no. 7, pp. 395–404. 1976.
[6] K. Sayood, Introduction to Data Compression, 2006.
[7] J. Miano, Compressed Image File Format, New York, 1999.
[8] M. Hans dan R.W. Schafer, "*Lossless* compression of digital audio," vol. 18, no. 4, pp. 21 - 32, 2001.
[9] Y.Q. Shi dan H. Sun, Image and Video Compression for Multimedia Engineering: Fundamentals, Algorithms, and Standards, Third Edition (Image Processing Series), 2019.
[10] L. L. Peterson dan B. S. Davie, Computer Network A System Approach, Morgan Kaufmann, 2007
[11] Microsoft, "Create a basic network diagram," [Online]. Available: https://support.office.com/en-us/article/create-a-basic-network-diagram-f2020ce6-c20f-4342-84f7-bf4e7488843a. [Diakses 21 11 2019]
[12] J. McCabe, Network Analysis, Architecture, and Design, 2007.
[13] Microsoft, "PowerShell," 17 08 2018. [Online]. Available: https://docs.microsoft.com/en-us/powershell/scripting/overview?view=powershell-6. [Diakses 21 11 2019].M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Tersedia: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/
[14] S. Academy, "SSH Protocol," [Online]. Available: https://www.ssh.com/ssh/protocol. [Diakses 16 Januari 2020].
[15] P. I. H. a. M. A. M. Luca Donetti, "Entangled Networks, Synchronization, and Optimal Network Topology," vol. 95, pp. 18-28, 2005.