

# BAB 1 PENDAHULUAN

## 1.1 Latar Belakang

Identifikasi trafik data pada layanan jaringan sangatlah penting guna pengelolaan dan pemantauan layanan jaringan yang baik. Identifikasi untuk mendeteksi trafik BitTorrent adalah salah satunya. BitTorrent merupakan aplikasi yang berjalan pada protokol P2P file sharing client. Jaringan P2P merupakan jaringan komputer dimana setiap komputer yang terhubung dalam jaringan tersebut merupakan klien sekaligus juga server. Penyedia Torrent yang beredar saat ini berjalan pada jaringan internet karena membutuhkan pengguna yang cukup banyak agar bisa melakukan aktivitas berbagi konten [1]. Pengguna yang berhasil mengunduh konten dari server Torrent disebut dengan peer. Seluruh peer akan saling berkontribusi untuk memberi pelayanan pada peer lainnya atau pengguna baru yang sedang mengunduh konten. Dengan menggunakan sistem file sharing BitTorrent akan mengurangi penggunaan pada server utama yaitu server BitTorrent dan dapat menghemat sumber daya. Namun beberapa organisasi melarang penggunaan BitTorrent karena mencuri sumber daya jaringan dan membuat kerentanan kebocoran data yang berdampak negatif bagi organisasi maupun individu [2]. Jika identifikasi trafik BitTorrent tidak ditindaklanjuti akan menyebabkan kehilangan ketersediaan server organisasi karena digunakan untuk memberi layanan ke pihak diluar organisasi.

Penelitian terdahulu yang membahas hal yang sama mengenai deteksi pada jaringan kampus adalah *Interception of P2P Traffic in a Campus Network*. Penelitian tersebut menyebutkan penggunaan lalu lintas masuk dan keluar P2P mencapai 10% untuk mengunggah dan 34% untuk mengunduh menggunakan bandwidth kampus [3]. Kejadian serupa terjadi pada jaringan publik IT Telkom Surabaya. Diduga trafik torrent tersebut ditemukan berasal dari pengguna aktif jaringan kampus yang berhasil mengunduh konten Torrent. Pengguna tersebut menjadi salah satu peer dalam *file sharing* BitTorrent. Peringkat penggunaan trafik BitTorrent pada jaringan kampus saat ini menjadi lima terbesar. Dampak P2P jika masuk lima besar adalah menghabiskan bandwidth jaringan yang seharusnya digunakan untuk kegiatan akademis dan penelitian. Hal ini dapat mengganggu

kinerja dan stabilitas jaringan kampus, serta membahayakan keamanan dan integritas data kampus karena kampus perlu menjamin keamanan jaringannya [4]. BitTorrent adalah protokol P2P yang memungkinkan pengguna untuk berbagi file besar dengan cepat dan efisien. Tetapi protokol ini juga menghasilkan lalu lintas yang tinggi dan tidak teratur, yang dapat mengganggu kinerja jaringan dan layanan lainnya. Selain itu, BitTorrent juga dapat membawa risiko keamanan, seperti penyebaran malware, pelanggaran hak cipta, dan pencurian data. Lima besar penggunaan trafik pada jaringan publik ITTelkom Surabaya dapat dilihat pada Gambar 1.1. Pada gambar tersebut peringkat P2P berada pada peringkat tiga. Pada umumnya penggunaan trafik menggunakan protokol HTTPS, UDP, dan HTTP. Tetapi ternyata diketahui penggunaan P2P dapat bersaing dari ketiga protokol yang umum digunakan.

App		App Group
No.	Name	
1	FileTransfer/HTTPS	
2	IP-PROTOCOL-GROUP/UDP-TRANSFERS	
3	P2P/P2P-DOWNLOAD-FLOW	
4	HTTP/HTTP-BROWSE	
5	HTTP/HTTP-Single-Threaded	

Gambar 1.1 Lima Besar Penggunaan Trafik Pada Jaringan Publik ITTelkom

Data tersebut diperoleh oleh admin jaringan Institut Teknologi Telkom Surabaya pada tahun 2022 dengan menggunakan aplikasi pemantauan jaringan. Urutan penggunaan *peer-to-peer* yang berada pada peringkat ketiga diperoleh pada saat jam kerja atau jam perkuliahan. Manfaat dan pengaruh deteksi BitTorrent pada ITTelkom Surabaya adalah untuk mengoptimalkan penggunaan bandwidth jaringan, meningkatkan kualitas layanan jaringan, dan mencegah potensi ancaman keamanan. Dengan menggunakan Snort sebagai deteksi BitTorrent, jaringan ITTelkom Surabaya dapat mengidentifikasi dan memblokir lalu lintas BitTorrent

yang tidak diinginkan [5]. Selain itu, dengan menggunakan bot Telegram sebagai monitoring jaringan, admin jaringan dapat memantau kondisi jaringan secara real-time dan mendapatkan notifikasi jika ada aktivitas mencurigakan atau pelanggaran kebijakan jaringan [6].

## **1.2 Rumusan Masalah**

Dari latar belakang masalah tersebut, peneliti merumuskan pertanyaan penelitian:

1. Bagaimana cara mendeteksi adanya BitTorrent ?
2. Bagaimana cara menampilkan notifikasi jika ditemukan trafik BitTorrent ?
3. Bagaimana mendesain topologi jaringan yang sesuai dengan kasus di ITTelkom Surabaya ?

## **1.3 Tujuan dan Manfaat**

### **1.3.1 Tujuan Penelitian**

Berdasarkan rumusan masalah yang dijabarkan, maka tujuan dari penelitian ini , yaitu:

1. Untuk mendeteksi trafik BitTorrent dilakukan implementasi dan analisis jaringan menggunakan perangkat lunak simulasi jaringan GNS3.
2. Pemberitahuan notifikasi dilakukan mengirim peringatan melalui aplikasi telegram jika ditemukan trafik BitTorrent .
3. Topologi yang digunakan adalah jaringan publik kampus secara umum. Topologi akan didesain untuk uji coba tindakan yang tidak diinginkan dari kegiatan torrent.

### **1.3.2 Manfaat Penelitian**

Mengenai manfaat dari penelitian ini, yaitu:

1. Mengurangi kerugian sumber daya komputasi dari trafik torrent.
2. Pemberitahuan jika terdapat trafik BitTorrent melalui aplikasi telegram.
3. Keamanan jaringan dari trafik BitTorrent.

4. Memberi ketersediaan trafik jaringan menjadi lebih besar.

#### **1.4 Batasan Masalah**

Batasan-batasan masalah pada penyusunan penelitian ini adalah sebagai berikut:

1. Kasus jaringan yang digunakan adalah jaringan ITTelkom Surabaya.
2. Metode deteksi yang digunakan menggunakan snort.
3. Jumlah pengguna torrent yang akan digunakan hingga 10 simulasi komputer.
4. Semua *Operating System*(OS) seperti pengguna, server snort, dan server BitTorrent akan menggunakan ubuntu.
5. Perangkat lunak simulasi jaringan yang digunakan adalah *Graphical Network Simulator 3*(GNS3).
6. Aplikasi yang digunakan untuk pemberitahuan ketika ditemukan trafik BitTorrent adalah aplikasi telegram.
7. Tidak melakukan implementasi pada jaringan fisik.

#### **1.5 Metodologi Penelitian**

Metode yang digunakan pada penelitian ini adalah metode NDLC. NDLC adalah singkatan dari Network Development Life Cycle, yaitu sebuah metode yang digunakan untuk merencanakan, mendesain, mengimplementasikan, dan memantau sistem jaringan komputer. NDLC berasal dari SDLC (*System Development Life Cycle*), yang merupakan teknik analisis terstruktur yang digunakan untuk mengembangkan sistem informasi. Dalam penyusunan karya tulis ini peneliti memperoleh data-data yang dibutuhkan menggunakan metode berikut.

##### **1.5.1 Metode Pengumpulan Data**

###### **1. Wawancara**

Wawancara dilakukan kepada narasumber untuk mendapatkan data-data dengan menanyakan tentang sesuatu kepada narasumber. Narasumber merupakan orang yang memiliki wewenang untuk mengelola jaringan kampus. Pembahasan yang ditanyakan adalah hal-hal yang berkaitan untuk penelitian.

## **2. Studi Literatur**

Studi literatur dilakukan dengan mencari referensi jurnal, buku, dan penelitian sebelumnya yang berkaitan dengan penelitian. Dengan cara tersebut peneliti mendapatkan data-data secara teoritis, informasi, dan konsep dari permasalahan yang sedang diteliti. Permasalahan tersebut berkaitan dengan BitTorrent, *Graphical Network Simulator 3*(GNS3), jaringan, keamanan siber, dan topologi. Informasi tersebut dapat penelitian gunakan sebagai pendukung didalam penelitian.

### **1.5.2 Metode Pengembangan Sistem**

Metode yang digunakan untuk melakukan pengembangan sistem adalah *Network Development Life Cycle*(NDLC). NDLC merupakan suatu siklus hidup pengembangan sistem jaringan komputer. Berikut tahapan-tahapan *Network Development Life Cycle*(NDLC) yang terdiri dari:

#### **1. Analisis Sistem**

Analisis sistem merupakan tahap awal untuk pengumpulan data, identifikasi masalah, pemecahan masalah, dan analisis kebutuhan sistem [7]. Hasil dari tahap ini akan menjadi dasar bagi tahap-tahap selanjutnya dalam proses pengembangan atau perancangan sistem jaringan.

#### **2. Perancangan Design**

Perancangan merupakan tahapan perancangan guna memenuhi kebutuhan untuk memecahkan masalah. Tahap perancangan menggunakan *logical design*. *Logical design* merupakan desain abstrak yang berisi informasi dan design digambarkan tidak detail seperti implementasi nyata.

#### **3. Simulation Prototype**

Simulasi prototipe merupakan tahapan menerapkan hasil dari perancangan. Tahap ini dilakukan dengan simulasi menggunakan perangkat lunak *Graphical Network Simulator 3*(GNS3).

#### **4. Implementation**

Tahap implementasi merupakan tahap melakukan kegiatan pengembangan yang telah dirancang. Tahap ini tetap menggunakan perangkat lunak simulasi *Graphical Network Simulator 3*(GNS3) dan virtualbox [8].

## **5. *Monitoring***

Tahap *monitoring* adalah tahap paling penting agar tetap menjaga jaringan komputer dan komunikasi agar sesuai dengan keinginan dan tujuan pengguna.

## **6. *Management***

Tahap manajemen merupakan tahapan mengelola jaringan agar dapat mendukung strategi bisnis. Membuat kebijakan terhadap layanan IT pada perusahaan bertujuan agar sistem yang telah dibangun dan berjalan dapat berlangsung lama dan unsur reliability terjaga. Tahap pengujian merupakan tahap uji coba sistem apakah telah berjalan sesuai yang telah direncanakan.