# BAB 1
# PENDAHULUAN

## 1.1 LATAR BELAKANG

Lalu lintas internet telah menarik penjahat siber dan menyebabkan banyak serangan siber di Indonesia. Otoritas Elektronik dan Mata Uang Kripto Nasional mencatat 495,3 juta serangan siber pada tahun 2020, meningkat 41% dibandingkan tahun sebelumnya 2019 sebanyak 290,3 juta. Begitu pula dengan Badan Reserse Kriminal Nasional (Bareskrim) yang mengalami peningkatan laporan kejahatan siber. Sementara itu, pada tahun 2019, sebanyak 4.586 laporan polisi disampaikan melalui Patrolisiber (situs pelaporan kejahatan siber Bareskrim), dibandingkan dengan 4.360 laporan pada tahun sebelumnya pada tahun 2018 BSSN telah mengidentifikasi berbagai potensi ancaman siber yang terjadi di Indonesia dan pada KTT G20(Nur Kumala Dewi1, 2021).

Ancaman tersebut antara lain *phishing online* (termasuk peretasan), dokumen berbahaya atau virus yang menempel pada dokumen, peretasan, *spoofing wifi* hingga membawa *malware* aktif kejahatan siber jenis ini tidak terjadi pada sistem operasi tertentu, namun semua jenis bisa tertular. Korban akan dirugikan karena data identitas penyerang digunakan untuk kepentingan pribadi dan merugikan orang lain. Salah satu tanda bahwa suatu perangkat berisiko terkena serangan mata uang kripto adalah kinerjanya yang lambat. Namun terkadang hal ini juga tidak dianggap sebagai serangan penjahat dunia maya yang serius. Salah satu kasus cryptojacking yang paling terkenal adalah "*WannaCry hack*". Kejahatan ini mempengaruhi hampir semua sistem di beberapa benua pada bulan Mei 2017. Hal ini terjadi pada serangan mata uang kripto, misalnya. Setidaknya ada dua cara bagi penyerang kriptografi untuk mendapatkan akses ke daya CPU perangkat korban. Yang pertama adalah memasukkan skrip enkripsi berbahaya ke perangkat target melalui tautan palsu. Hal ini dapat dilakukan melalui berbagai metode, salah satu yang paling umum adalah penggunaan *email phishing*. Cara kedua adalah bagi peretas untuk menyematkan skrip berbahaya di situs *web populer*. Setiap perangkat yang mengakses situs web secara otomatis melakukan penambangan *cryptocurrency*. Selain *website*, *hacker* juga kerap memanfaatkan iklan yang muncul di browser. Jika korban mengklik iklan yang *terinfeksi*, *skrip*

dijalankan secara otomatis. Tanda-tanda serangan ini termasuk peningkatan penggunaan CPU, koneksi *internet*, dll. Di antara aktivitas anomali tersebut di atas, salah satu jenis serangan yang ada adalah penggunaan sumber daya ilegal (*hi-security*/*verifikasi* pelanggaran). uang elektronik. Bentuk kejahatan ini dapat menargetkan konsumen *individu*, organisasi besar, dan bahkan sistem kontrol industri. Berdasarkan *konteks* di atas. Penelitian ini akan menganalisis lalu lintas jaringan dengan metode pengumpulan data langsung, yang dilakukan untuk menganalisis anomali lalu lintas data. Hasil penelitian ini kemudian dilakukan untuk mengumpulkan data yang terkumpul sebagai bukti digital untuk keperluan *DFIR* (*Digital Forensic and Incident Response*)(Slamet, 2018).

## 1.2 PERUMUSAN MASALAH

Dilihat dari latar belakang dijelaskan maka rumusan masalah dari penelitian ini adalah sebagai berikut :

1. Bagaimana sistem *maltrail* dapat mendeteksi ketidak normalan atau perilaku lau lintas jaringan yang tidak biasa yang mungkin berasal dari *cryptomining*?
2. Bagaimana cara mendapatkan bukti anomali jaringan dalam *cryptomining* berdasarkan hasil pengujian ?

## 1.3 PERTANYAAN PENELITIAN

1. Bagaimana cara mengetahui lalu lintas jaringan yang berjalan dalam *mining data*?
2. Bagaimana mendapatkan bukti anomali jaringan ?
3. Apa solusi yang bisa direkomendasikan untuk hasil anomali lalu lintas jaringan dalam *cryptomining*?

## 1.4 TUJUAN PENELITIAN

1. Mengidentifikasi anomali jaringan untuk mendapatkan bukti dalam mining aplikasi *verus* .
2. Mengetahui hasil penilaian dan analisis menggunakan *Mailtrail* .
3. Bagaimana penerapan penggunaan *Maltrail* untuk me-*monitoring* lalu lintas jaringan?

## 1.5 MANFAAT HASIL PENELITIAN

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Merancang dan membangun system monitoring jaringan dengan menggunakan *Maltrail*
2. Menambah ilmu pengetahuan mengenai penilaian lalu lintas jaringan dalam aplikasi berbasis saham dan mata uang.
3. Dapat *mengimplementasikan* ilmu baru mengenai *mailtrail*.