1. Pendahuluan

1.1 Latar Belakang

Penggunaan Internet meningkat secara drastis dalam 10 tahun belakangan ini **[9]**. Namun tidak bisa dipungkiri juga bahwa ada banyak sisi negatif dari Internet, sebut saja *hacking, abuse, cracking, carding* dan sebagainya. Kejahatan di dunia maya yang semakin marak ini tidak dibarengi dengan hukum yang baik, bahkan tidak ada pasal-pasal yang bisa digunakan untuk menghukum pelakunya.**[3]**

Computer forensic merupakan suatu cabang ilmu yang bisa digunakan untuk menganalisa dan mengidentifikasi kejahatan yang dilakukan di dunia maya. Salah satu bagian dari computer forensic ini adalah log forensic. Dari log file ini bisa didapatkan bukti yang bisa digunakan untuk menganalisa berbagai hal, mulai dari serangan pada komputer, firewall, internetworking device, dan juga perangkat korban lainnya **[4].**

Kebanyakan pembacaan log file untuk log forensik dilakukan secara manual dengan membacanya per baris satu per satu file yang telah dibaca dan dikonversi menjadi suatu file yang bisa dibaca oleh manusia. Dalam penelitian ini, forensic akan dilakukan secara offline, dimana data log yang akan dianalisis adalah log files yang telah ada dan bukan saat sistem telah berjalan. Log yang telah diambil tersebut akan dianalisa dengan menggunakan metode Recurrent Neural Network (RNN). Dari faktor performansi juga disebutkan bahwa RNN bisa mengurangi waktu dan cost dari forensic yang dilakukan.**[1]**

RNN sendiri merupakan suatu cabang dari Artificial Neural Network yang dibuat untuk meniru cara kerja otak manusia dan memiliki kemampuan untuk belajar (learning) dan mengekstrak informasi dari suatu urutan input untuk menghasilkan klasifikasi ada tidaknya serangan pada jaringan. Dikatakan juga bahwa RNN ini merupakan suatu algoritma yang otomatis dan efektif untuk analisis forensik pada jaringan. **[1]**

Analisis yang akan dilakukan adalah untuk mencari akurasi dari RNN dalam mendeteksi serangan pada jaringan, sehingga bisa disimpulkan baik tidaknya metode ini.

1.2 Perumusan Masalah

Dengan latar belakang yang telah disebutkan sebelumnya, maka masalah yang dapat diangkat adalah sebagai berikut

1. Bagaimana memproses log file yang telah ada dengan metode RNN agar bisa digunakan untuk keperluan forensic
2. Bagaimana arsitektur RNN yang baik untuk log analisis sehingga didapat hasil akurasi yang paling bagus
3. Parameter apa saja yang mempengaruhi akurasi yang didapat dari segi forensic

Dari perumusan masalah di atas, maka disusun juga batasan masalah yang akan ditangani yaitu:

1. Analisis dilakukan secara offline, bukan saat system sedang berjalan

2. Log yang akan dianalisis adalah log router yang telah ada dan sudah jelas bagian mana yang merupakan serangan dan yang bukan untuk penghitungan akurasinya

1.3 Tujuan

Berdasarkan perumusan masalah, maka tujuan pembuatan tugas akhir ini adalah:

1. Untuk mengetahui cara memproses log files yang telah ada dengan metode RNN sehingga bisa digunakan untuk keperluan forensic
2. Untuk mengetahui arsitektur RNN yang baik dan menghitung akurasi metode RNN yang digunakan untuk melakukan log analisis
3. Mengetahui parameter-parameter yang mempengaruhi akurasi yang didapat dari segi forensic

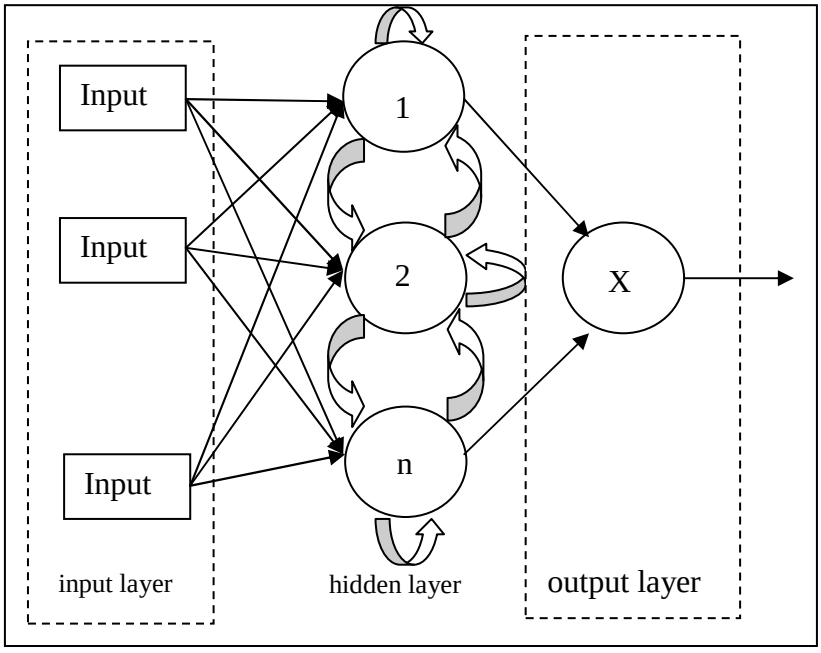
1.4 Metodologi Penyelesaian Masalah

Metode penelitian yang akan digunakan guna menyelesaikan permasalahan yang ada adalah sebagai berikut :

1. Tahap studi literatur
   Literatur utama yang digunakan dalam penelitian ini adalah *Neural Network Based Attack Detection Algorithm* yang menyatakan bahwa algoritma yang diajukan untuk melakukan suatu network analysis adalah recurrent neural network yang bisa menganalisa serangan pada jaringan computer dan bisa melakukan klasifikasi yang mana merupakan serangan dan yang mana yang bukan serta memberikan baris dari log tersebut yang merupakan serangan jika ada yang dalam paper ini disebut sebagai **evidence extraction**, algoritma ini juga bisa menyingkat waktu dan cost untuk forensic. Untuk konsep network forensic sendiri mengacu pada buku *Computer Forensic for Dummies* yang menjelaskan konsep computer forensic mulai dari dasarnya, serta untuk beberapa literature yang mendukung dalam melakukan forensic itu sendiri seperti *Computer Hacking Forensic Investigator* yang juga menjelaskan tentang konsep dan cara-cara melakukan forensic, namun yang diambil hanya di bagian modul *XIX: Network Forensic* dan *XXIII: Router Forensic* serta *Network Forensic: Log Analysis* untuk lebih mengerti tentang konsep log analysis itu sendiri. Sementara untuk contoh lain yang melakukan log analysis digunakan *Cisco Pix Log Analysis In a University Setting* dimana menjelaskan secara detail bagaimana melakukan Log Analysis secara lengkap dengan setting di dalam suatu Universitas dengan scenario tertentu. Untuk mempelajari teknik-teknik dan tools yang digunakan dalam network forensic yang bisa ditemukan dalam literature yang berjudul *Tools dan Techniques for Network Forensic.*
   Untuk metodenya sendiri yaitu RNN dikumpulkan beberapa literature lain sebagai sumber. Ada literature yang digunakan dalam perkuliahan di IT Telkom sendiri yaitu *Soft Computing* sebagai dasar pembelajaran untuk

ANN. Untuk konsep RNN sendiri dibahas secara cukup terperinci dalam *A Guide to Recurrent Neural Network dan Backpropagation*.

2. Tahap pengumpulan data
   Pada tahap ini akan dilakukan pengumpulan data berupa log file dari router yang telah. Log yang dikumpulkan ada log yang sudah dianalisa sehingga jelas bagian mana yang serangan dan yang bukan sebagai ukuran untuk akurasi dari penelitian yang akan dilakukan.
3. Analisis dan Perancangan Sistem
   Pada tahap ini akan dilakukan analisis terhadap hal-hal yang bisa menunjang pembangunan system. Secara umum system yang dibangun akan terdiri dari beberapa tahapan yaitu:
   - Pembuatan prosedur pembacaan log file
   - Pembagian data
   - Preprocessing, yaitu proses untuk mengkomposisikan input sebagai masukan untuk RNN.
   - Pengaplikasian metode RNN dalam pembuatan system, dimana arsitektur RNN **secara umum** digambarkan sebagai berikut:



*Gambar 1. Contoh Arsitektur RNN **[1]***

   - Memasukkan data yang telah diubah ke numeric pada preprocessing sebelumnya ke dalam system RNN yang telah dibangun
   - Penghitungan akurasi dan performansi system
4. Tahap pembuatan sistem
   Pada tahap ini akan dilakukan pembuatan system analisis log dengan metode RNN (Recurrent Neural Network) yang menggunakan bahasa pemrogramana matlab.
5. Tahap pengujian sistem
   Pada tahap ini akan dilakukan pengujian terhadap sistem yang dibangun dengan memberikan data dari sislog yang telah dipilah menjadi data training

dan data testing dan juga dilakukan pembandingan hasil dari aplikasi dengan hasil log forensic secara manual.

6. Tahap dokumentasi
   Tahap dokumentasi dilakukan mulai dari pengumpulan data sehingga semua tahapan akan terdokumentasi dengan jelas