# BAB 1

# PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi menimbulkan pertumbuhan yang pesat pada penggunaan media sosial. Media sosial memudahkan interaksi antar pengguna menggunakan teknologi internet. Media sosial memiliki peran penting sebagai alat penyebaran informasi mengenai seseorang maupun suatu brand yang ada. Sehingga semua orang mencoba untuk memperoleh seluruh atensi yang ada pada suatu platform seperti *Instagram*. *Instagram* membatasi para *influencer* dengan memberikan tanda verifikasi pada akun *influencer*.

Namun perkembangan media sosial memiliki dampak negatif seperti penipuan akun, pencurian data pribadi, dan penjualan akun yang telah diretas oleh peretas atau *hacker*. Selain hal yang peneliti sebutkan masih terdapat banyak jenis kasus kejahatan yang dilakukan oleh para peretas tersebut.

C*yber crime* marak terjadi di aplikasi media sosial, penyidik harus melakukan pengolahan barang bukti digital dengan teknik forensik terhadap perangkat yang dimiliki korban maupun tersangka untuk menemukan barang bukti tindak kejahatan (Aziz et al., 2018). Jenis kejahatan yang sering terjadi adalah *Phishing* yaitu penipuan yang seolah menampilkan keorisinilan dan keamanan data yang seharusnya dilakukan dalam suatu jaringan internet (Mushlihudin & Nofiyan, 2020).

Pada tahun 2021 setidaknya terjadi 264 kasus *phishing* yang berhasil dicatat oleh BSSN Indonesia. Berdasarkan data tahunan BSSN *phishing* dibagi menjadi 5 jenis, yaitu: *Email Phishing*, *Spear Phishing, Whaling, Vishing,* dan *Smishing.* Kejahatan ini dapat menimbulkan kerugian yang nyata karena data korban dapat digunakan untuk melakukan tindakan

negatif seperti mencuri dengan mengatasnamakan korban, meretas sistem komputer, hingga tindakan lainnya yang merugikan dari sisi keamanan.

Digital forensik adalah ilmu pengetahuan yang berfungsi untuk membantu hukum (Ayunita Kinasih et al., 2020). Digital forensik memudahkan pencarian informasi penting terkait barang bukti digital yang akan memberatkan maupun melemahkan pidana yang hendak dijatuhkan dalam suatu kasus kejahatan. Metode yang dapat digunakan dalam ilmu digital forensik telah diusulkan oleh *National Institute of Justice* (NIJ). Dalam memudahkan investigasi terkait pelaku, kita bisa melakukan pelacakan berdasarkan IP address dan DNS pelaku.

Dalam penulisan skripsi ini, penulis akan melakukan analisis terhadap barang bukti (.pcap) menggunakan *tools Wireshark* untuk mengolah data yang telah di*capture* dan menemukan barang bukti digital yang mengarah pada penyebab kasus kejahatan tersebut terjadi.

## 1.2. Identifikasi Masalah

Identifikasi masalah yang ada sebagaimana telah dijelaskan di latar belakang penelitian ini, adalah sebagai berikut:

1. Banyaknya tindak kejahatan siber (*cyber crime*) yang terjadi.
2. Sulitnya menemukan penyebab akun diretas.

## 1.3. Rumusan Masalah

Rumusan masalah yang terdapat dalam penelitian ini, yaitu:

1. Apakah dengan menggunakan metode *National Institute of Justice* dalam Digital Forensik dapat mengetahui penyebab kejahatan *spear phishing*?
2. Apakah identitas pelaku kejahatan *spear phishing dapat diketahui?*
3. Bagaimana proses investigasi penyerangan *spear phishing*?
4. Apa sajakah data yang didapatkan dari hasil analisis barang bukti *spear phishing?*

## 1.4. Batasan Masalah

Batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Jenis *Phishing* yang akan diteliti hanyalah *Spear Phishing.*
2. Penelitian ini menggunakan Sistem Operasi Windows 10, tools yang digunakan antara lain Wireshark, NetworkMiner, WHOIS, dan Central OPS.
3. Analisis dilakukan berdasarkan metode *National Institute of Justice* (NIJ)
4. Penelitian hanya berfokus pada *Spear Phishing* terkait media sosial *Instagram*.
5. Penelitian hanya berfokus pada *protocol HTTP.*

## 1.5. Tujuan Penelitian

Tujuan yang hendak dicapai dari penelitian ini adalah mengimplementasikan analisis digital forensik terhadap barang bukti tindak kejahatan *spear phishing* dengan investigasi log file Wireshark.

## 1.6. Manfaat Penelitian

Manfaat yang didapat dari penelitian ini adalah sebagai berikut:

1. Untuk peneliti, dapat melakukan analisis forensik kejahatan *spear phishing* untuk mencari penyebab akun diretas.
2. Untuk akademis, sebagai acuan referensi untuk penelitian terkait *spear phishing* dan implementasi Digital forensik menggunakan metode *National Institute of Justice*.
3. Untuk masyarakat, sebagai edukasi terkait mudahnya kejahatan siber *spear phishing* terjadi dan cara untuk menghindarinya.

## 1.7. Sistematika Penulisan

Sistematika penulisan skripsi Analisis Digital Forensik *Spear Phishing* Menggunakan Metode *National Institute of Justice* (NIJ) Studi Kasus: Instagram, yaitu:

**BAB 1 PENDAHULUAN**

Pada bagian ini peneliti akan menjelaskan secara singkat dan jelas mengenai latar belakang permasalahan, rincian permasalahan, tujuan diadakannya penelitian, manfaat yang dapat diraih dari penelitian, dan sistematika yang digunakan selama penulisan.

**BAB 2 TINJAUAN PUSTAKA**

Bagian ini akan berisi mengenai uraian berbagai literatur yang berkaitan baik dari segi teori maupun konsep mengenai metode atau proses yang digunakan selama penelitian yaitu mengenai analisis digital forensik.

**BAB 3 METODOLOGI PENELITIAN**

Pada bagian metodologi penelitian akan berisi tentang tahapan-tahapan yang nantinya digunakan oleh peneliti berdasarkan metode yang sudah diusulkan dalam penelitian ini.

**BAB 4 PEMBAHASAN**

Bagian ini akan berisi mengenai penjelasan tentang segala proses yang diimplementasikan dalam pengujian, serta hasil yang didapat dari penelitian.

**BAB 5 PENUTUP**

Pada bagian penutup penelitian ini akan berisi mengenai kesimpulan dan saran yang dibuat berdasarkan pembahasan masalah dan hasil yang ditemukan dalam penelitian yang telah dilakukan. Dimana saran tersebut diharapkan dapat digunakan sebagai acuan dalam pengembangan penelitian selanjutnya terkait *spear phishing*.