BAB 5

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dari penelitian yang telah dilakukan, mengenai penggunaan metode *National Institute of Justice* terhadap *evidence SpearPhishingInstagram* didapatkan beberapa informasi yang dapat disimpulkan sebagai berikut :

1. Pengaplikasian metode NIJ yang dibantu dengan tools Wireshark dan NetworkMiner dapat mengetahui penyebab mengapa korban mengalami kejahatan ini dikarenakan korban mengklik suatu laman atau pranala yang telah dibuat oleh pelaku kejahatan.
2. Identitas pelaku kejahatan tidak berhasil didapatkan berdasarkan referensi dari Domain yang digunakan pelaku karena tidak terdaftar pada database Who.is maupun Central OPS, dan IP Address yang digunakan pelaku karena bersifat dinamis. Informasi yang ditemukan hanya informasi terkait perusahaan dimana pelaku melakukan hosting laman penipuan dalam tindak kejahatan tersebut.
3. Berdasarkan penelitian yang dilakukan, proses investigasi penyerangan *spear phishing* dilakukan dalam beberapa tahapan atau cara seperti *Preparation, Collection, Examination, Analysis,* dan *Reporting* sesuai dengan metode yang telah diusulkan oleh pihak *National Institute of Justice* (NIJ) dengan tindak lanjut analisis barang bukti yang didapat.
4. Dari hasil pengolahan data yang dianalisis didapatkan bahwa :

- Pelaku kejahatan menggunakan protokol http sebagai protokol untuk mengambil data atau file pada laman penipuan milik pelaku. Maka dapat digunakan fitur filtrasi yang disediakan oleh aplikasi Wireshark berupa *tcp.port == 80 || udp.port == 80* guna mempermudah analisis.
- Di dalam paket pengiriman yang dianalisis pelaku melakukan redirecting laman palsu miliknya ke laman asli milik Instagram untuk menghilangkan kecurigaan korban.

- Pelaku menggunakan IP Address cukup beragam yang bergantung pada siapa target yang ingin diincar oleh pelaku dan pelaku menggunakan hosting laman yang memiliki IP bersifat dinamis sehingga sulit untuk dilakukan pelacakan terkait tindak kejahatan tersebut.

5.2 Saran

Adapun saran yang dapat diberikan oleh peneliti untuk pencegahan dan penanggulangan kasus *phishing* terutama *spear phishing* yang dapat dilakukan lebih mengarah kepada edukasi masyarakat untuk tidak mengklik *link* atau laman yang tidak dikenal. Tidak memasukkan informasi kredensial seperti username maupun password pada situs yang tidak dikenal.

Terkait pengembangan penelitian selanjutnya diharapkan dapat menggunakan tools yang lebih memadai dalam pendekripsian lalu lintas jaringan. Melakukan proses *capture* data melalui suatu jaringan secara menyeluruh melalui berbagai *device* dan lebih memperdalam pengusutan pencarian informasi terkait pelaku tindak pidana, tidak hanya mengandalkan aplikasi seperti WHOIS dan Central OPS .