TESIS

PELACAKAN PELAKU KEJAHATAN SIBER PENGGUNA *VIRTUAL PRIVATE NETWORK* (VPN) PADA JARINGAN *THE ONION ROUTER* (TOR)

(Studi Kasus di Badan Siber dan Sandi Negara)

Oleh

Muh. Abduh Dwi Putra
NIM 091714653003

PROGRAM STUDI MAGISTER
ILMU FORENSIK
SEKOLAH PASCASARJANA
UNIVERSITAS AIRLANGGA
SURABAYA
2020

TESIS

PELACAKAN PELAKU KEJAHATAN SIBER PENGGUNA *VIRTUAL PRIVATE NETWORK* (VPN) PADA JARINGAN *THE ONION ROUTER* (TOR)

(Studi Kasus di Badan Siber dan Sandi Negara)

Oleh

Muh. Abduh Dwi Putra
NIM 091714653003

PROGRAM STUDI MAGISTER
ILMU FORENSIK
SEKOLAH PASCASARJANA
UNIVERSITAS AIRLANGGA
SURABAYA
2020

TESIS

PELACAKAN PELAKU KEJAHATAN SIBER PENGGUNA *VIRTUAL PRIVATE NETWORK* (VPN) PADA JARINGAN *THE ONION ROUTER* (TOR)

(Studi Kasus di Badan Siber dan Sandi Negara)

Untuk Memenuhi Syarat Memperoleh Gelar Magister
Dalam Program Studi Ilmu Forensik
Pada Sekolah Pascasarjana Universitas Airlangga

Oleh

Muh. Abduh Dwi Putra
NIM 091714653003

SEKOLAH PASCASARJANA
UNIVERSITAS AIRLANGGA
SURABAYA
2020

Lembar Pengesahan

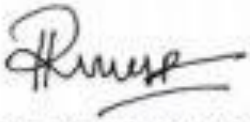
TESIS INI TELAH DISETUJUI
PADA TANGGAL 23 JANUARI 2020

Oleh:

Pembimbing Ketua

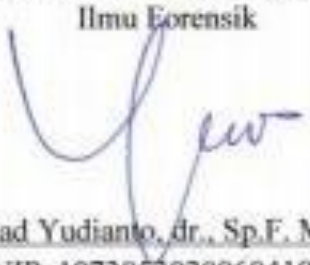
Prof. Dr. Retna Apsari, M.Si
NIP. 196806261993032003

Pembimbing Kedua



Dr. Riries Rulaningtyas S.T., M.T.
NIP. 197903152003122002

Mengetahui,
Koordinator Program Studi Program Magister
Ilmu Forensik



Dr. Ahmad Yudianto, dr., Sp.F. M.Kes., SH
NIP. 197305302006041019

Telah diuji pada

Tanggal : 20 Januari 2020

PANITIA PENGUJI TESIS

Ketua : Prof. Dr. Ir. Suhariningsih

Anggota : 1. Prof. Dr. Retna Apsari, M.Si

2. Dr. Riries Rulaningtyas S.T., M.T.

3. Dr. Ahmad Yudianto, dr., Sp.F(K). M.Kes., SH

4. Dr. Suryani Dyah Astuti, S.Si., M.Si.

PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Muh. Abduh Dwi Putra
NIM : 091714653003
Program Studi : Magister Ilmu Forensik
Judul Tesis : Pelacakan Pelaku Kejahatan Siber Pengguna *Virtual Private Network* (VPN) Pada Jaringan *The Onion Router* (TOR) (Studi Kasus di Badan Siber dan Sandi Negara).

Menyatakan dengan sebenarnya bahwa Tesis saya ini adalah asli (hasil karya sendiri) bukan merupakan hasil peniruan atau penjiplakan (*Plagiarism*) dari karya orang lain. Tesis ini belum pernah diajukan untuk mendapatkan gelar akademik.

Dalam tesis ini tidak terdapat pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dengan disebutkan nama pengarang dan dicantumkan di dalam daftar pustaka. Demikian, pernyataan ini dibuat tanpa adanya paksaan dari pihak manapun, apabila pernyataan ini tidak benar, maka saya bersedia menerima sanksi sesuai dengan norma dan peraturan yang berlaku di Universitas Airlangga.

Surabaya, 23 Januari 2020

Muh. Abduh Dwi Putra
NIM. 091714653003

UCAPAN TERIMA KASIH

Puji syukur Kehadirat Allah SWT atas karunia yang telah dilimpahkan sehingga penulis dapat melaksanakan penelitian dan menyelesaikan tesis dengan judul PELACAKAN PELAKU KEJAHATAN SIBER PENGGUNA *VIRTUAL PRIVATE NETWORK* (VPN) PADA JARINGAN *THE ONION ROUTER* (TOR) (STUDI KASUS DI BADAN SIBER DAN SANDI NEGARA).

Saya menyadari bahwa tanpa bantuan dan bimbingan berbagai pihak mulai dari perkuliahan hingga penyusunan tesis ini, sulit bagi saya bisa menyelesaikan tesis ini dengan baik. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih kepada:

1. Direktur Sekolah Pascasarjana Universitas Airlangga, Prof. Dr. Hj. Sri Iswati, SE., M.Si., Ak., Wakil Direktur I, Prof. Dr. Anwar Ma'ruf, drh., M.Kes, Wakil Direktur II, Dr. Dina Sunyowati, S.H., M.Hum. atas kesempatan dan dukungannya bagi penulis dalam mengikuti pendidikan di Program Studi Magister Ilmu Forensik Sekolah Pascasarjana Universitas Airlangga.
2. Dr. Ahmad Yudianto, dr., Sp.F(K), M.Kes., SH selaku Koordinator Program Studi Magister Ilmu Forensik Sekolah Pascasarjana Universitas Airlangga atas bimbingan dan dukungannya kepada penulis sejak menjadi mahasiswa hingga akhirnya penulis dapat menyelesaikan tesis ini dengan baik.
3. Prof. Dr. Retna Apsari, M.Si selaku Pembimbing Ketua yang selalu membimbing, menginspirasi, berbagi ilmu dan pengalaman serta memberi semangat kepada penulis sehingga penulis mampu menyelesaikan studi dengan baik.

4. Dr. Riries Rulaningtyas S.T., M.T. selaku Pembimbing Serta atas waktu yang berharga dalam membimbing penulis dan berbagi ilmu serta pengalaman sehingga penulis dapat menyelesaikan penelitian ini dengan baik.
5. Prof. Dr. Ir. Suhariningsih dan Dr. Suryani Dyah Astuti, S.Si., M.Si. selaku Penguji penulis yang senantiasa memberi ide-ide, saran dan masukan agar penulis dapat membuat suatu penelitian yang lebih baik.
6. Bapak Sulistyo, S.Si., S.T., M.Si. selaku Direktur Direktorat Deteksi Ancaman, Ibu Pinuji Prasetyaningtyas selaku Kepala Subdirektorat Forensik Digital dan Analisis Kripto, Risky Yugitama selaku staf Subdirektorat Deteksi Serangan Siber, Pak Johan, Pak Basuki, Pak Deka, dan seluruh pihak instansi BSSN yang tidak bisa penulis sebutkan satu-persatu atas waktu, informasi dan segala bantuannya dalam pengumpulan data penelitian ini.
7. Seluruh staf pengajar Magister Ilmu Forensik yang tidak dapat penulis sebutkan satu-persatu atas warisan keilmuannya selama penulis menempuh studi di Magister Ilmu Forensik Sekolah Pascasarjana Universitas Airlangga.
8. Kedua orang tua, adik-adik, dan keluarga penulis atas kasih sayang, dukungan, kepercayaan, bantuan materiil dan doa hingga penulis dapat menyelesaikan studi dengan baik.
9. Seluruh staf pegawai Sekolah Pascasarjana, baik staf Akademik, staf Bagian Umum, staf TU, staf Keuangan, staf DSI, dan semuanya yang berada di lingkungan Sekolah Pascasarjana yang tidak dapat penulis sebutkan satu persatu. Terima kasih atas segala bantuan selama saya menempuh studi di Sekolah Pascasarjana.

10. Teman-teman penulis semuanya yang tidak bisa disebutkan satu persatu.

Sukses selalu dan terus bersinergi membangun negeri.

Surabaya, 23 Januari 2020

Penulis

RINGKASAN

Pelacakan Pelaku Kejahatan Siber Pengguna *Virtual Private Network* (VPN) pada Jaringan *The Onion Router* (TOR) (Studi Kasus di Badan Siber dan Sandi Negara)

Muh. Abduh Dwi Putra

Seiring dengan maraknya kasus kejahatan siber di Indonesia, maka keamanan data pada jaringan internet juga semakin diperhatikan. Hingga saat ini, terkait keamanan *online*, *Virtual Private Network* (VPN) dan *The Onion Router* (TOR) adalah alat yang paling ampuh. Namun muncul suatu fenomena di mana kedua teknologi dapat disalahgunakan oleh pelaku kejahatan siber untuk melakukan serangan siber, dengan maksud agar mereka sulit dilacak oleh pihak berwenang ketika mereka melakukan aksinya. Oleh sebab itulah penulis bermaksud ingin meneliti mengenai prosedur dan strategi yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN), sebagai salah satu lembaga yang berwenang dalam *cyber security* di Indonesia, dalam melakukan pelacakan pelaku kejahatan siber di Indonesia yang menggunakan VPN pada jaringan TOR khususnya pada kasus ancaman teror melalui *Facebook messenger*, *WhatsApp,* dan *e-mail*.

Penelitian ini bersifat deskriptif dengan metode kualitatif. Teknik pengumpulan data adalah dengan observasi, wawancara dan dokumentasi. Teknik pengambilan sampel yaitu menggunakan *purposive sampling*. Penelitian dilakukan di instansi BSSN, pada Deputi Bidang Identifikasi dan Deteksi dan Deputi Bidang Pemantauan dan Pengendalian. Penelitian dimulai dengan melakukan pengamatan terhadap dokumen penunjang seperti regulasi dan Standar Operasional Prosedur (SOP) yang berlaku. Kemudian penulis melakukan wawancara kepada beberapa narasumber yang mewakili setiap unit kerja serta menggunakan kuesioner untuk staf teknis juga pada masyarakat terkait pengetahuan tentang VPN dan TOR. Dalam wawancara teknis, penulis berdiskusi mengenai pelacakan pada pelaku kejahatan siber berupa ancaman teror berisi pesan, yang telah disematkan virus, yang dikirim melalui *Facebook*, *WhatsApp messenger,* dan *e-mail*. Minimal parameter yang dilihat adalah lokasi alamat IP pelaku, atau kode MAC perangkat, atau asal jaringan/ISP dari pelaku tersebut. Hasil pengamatan, wawancara serta kuesioner dikumpulkan dan didokumentasikan.

Berdasarkan hasil observasi, dan wawancara, diketahui bahwa regulasi masih bersifat atribusi dan masih berlandaskan Perpres, menunggu sahnya RUU KKS, sehingga regulasi tertinggi masih berupa Pedoman Kepala BSSN dan Peraturan BSSN. SOP masih berupa juknis internal dan belum adanya regulasi yang kuat sehingga menyebabkan terbatasnya kewenangan BSSN dalam investigasi pelaku kejahatan siber.

Berdasarkan hasil kuesioner teknis dan masyarakat, dapat diukur beberapa hal antara lain staf BSSN diharuskan selalu *up to date* dengan perkembangan

teknologi khususnya VPN & TOR; 76,9% dari 130 responden masyarakat telah mengetahui tentang VPN & TOR, walaupun 80 responden di antaranya belum pernah menggunakannya; SOP belum spesifik terkait pelacakan pelaku kejahatan siber pengguna VPN dan TOR; dan kasus yang banyak ditangani oleh BSSN adalah terkait ujaran kebencian dan provokasi, khususnya yang disebarkan melalui media sosial.

Penulis merangkum dari seluruh hasil di atas, bahwa metode dan strategi BSSN dalam menangani serangan siber antara lain dengan membentuk Gov-CSIRT dan Pusopskamsinas; menggunakan *Honeynet* sebagai sistem deteksi dini serangan siber; melakukan serangan balik terhadap pelaku dan berkoordinasi dengan penegak hukum.

Langkah respon BSSN dalam menangani serangan ancaman teror yang masuk ke jaringan BSSN yaitu serangan tersebut akan mengaktifkan sensor *Honeypot*, kemudian sinyal bahaya tersebut terekam dalam *log Honeypot*. Dionaea yang ada dalam sensor *Honeypot* akan menganalisa sumber serangan sehingga akan terlacak alamat IP pelaku dari *path* terakhir yang dilalui serta *timestamp*. Hasil ini akan divisualisasikan dalam website *Honeynet* BSSN, kemudian dilakukan pelacakan alamat IP, analisis jaringan yang digunakan pelaku hingga didapatkan alamat IP pelaku.

Berdasarkan analisa penulis, pelaku kejahatan siber yang menggunakan VPN dan TOR dapat terlacak oleh karena adanya kebocoran DNS dan WebRTC, perpindahan relai TOR yang terdeteksi, dan simpul keluar TOR yang tidak terenkripsi.

Untuk mengisi keterbatasan wewenang BSSN dalam melacak pelaku kejahatan siber, khususnya yang melakukan serangan melalui akun media sosial yang menggunakan VPN dan TOR, maka penulis merancang dan merekomendasikan kepada BSSN suatu *project profiling* untuk masing-masing media sosial yang digunakan dengan memanfaatkan informasi yang dapat digali dari profil akun tersebut.

Hambatan yang ditemukan dalam penelitian ini yaitu terkait prosedural, keterbatasan waktu dalam penelitian, keterbatasan SDM BSSN dan kebijakan BSSN terkait dokumentasi dan kerahasiaan data. Rekomendasi yang penulis berikan untuk BSSN yaitu mengenai penerbitan SOP pelacakan pelaku kejahatan siber pengguna VPN dan TOR dan SOP profiling pada akun media sosial serta perumusan kebijakan terkait penggunaan media sosial untuk investigasi.

Kesimpulan dari penelitian ini adalah *project profiling* melalui akun media sosial dapat membantu proses pelacakan pelaku kejahatan siber pengguna VPN dan TOR di instansi BSSN dengan tetap berkoordinasi dengan aparat penegak hukum.

SUMMARY

TRACKING CYBER CRIMINALS OF VIRTUAL PRIVATE NETWORK (VPN) USERS ON THE ONION ROUTER (TOR) NETWORK (CASE STUDY AT NATIONAL CYBER AND CRYPTO AGENCY)

Muh. Abduh Dwi Putra

Along with the rise of cybercrime cases in Indonesia, data security on the internet network is also increasingly being considered. Until now, regarding online security, Virtual Private Network (VPN) and The Onion Router (TOR) are the most powerful tools. However, there is a phenomenon where both technologies can be misused by cyber criminals to carry out cyber attacks, with the intention that they are difficult to be tracked by the authorities when they carry out the action. That is why the author intends to examine the procedures and strategies carried out by Badan Siber dan Sandi Negara (BSSN), as one of the institutions authorized in cyber security in Indonesia, in tracking cybercrime perpetrators in Indonesia who use VPN on the TOR network especially in cases of terror threats through Facebook messenger, WhatsApp and e-mail.

This research is descriptive with qualitative methods. Data collection techniques are by observation, interview and documentation. The sampling technique is using purposive sampling. The study was conducted at the BSSN agency, at the Deputy for Identification and Detection and the Deputy for Monitoring and Control. The study began by observing supporting documents such as regulations and applicable Standard Operating Procedures (SOPs). Then the authors conducted interviews with several speakers representing each work unit and used a questionnaire for technical staff as well as the community related to knowledge about VPN and TOR. In a technical interview, the author discusses tracking on cyber crime perpetrators in the form of terror threats containing messages, which have been pinned viruses, sent via Facebook, WhatsApp messenger, and e-mail. The minimum parameters to be seen are the location of the IP address, or MAC address of the device, or the origin of the network / ISP of the offender. Observations, interviews and questionnaires are collected and documented.

Based on observations and interviews, it is known that the regulations are still attributable and are still based on Perpres, awaiting the validity of the RUU KKS, so that the highest regulations are still in the form of Guidelines for the Head of BSSN and BSSN Regulations. SOP is still in the form of internal technical guidelines and the absence of strong regulations which causes the limited authority of BSSN in investigating cyber crime perpetrators

Based on the results of technical and community questionnaires, several things can be measured, among others, BSSN staffs are required to be always up to date with technological developments, especially VPN & TOR; 76.9% of 130 community respondents already know about VPN & TOR, although 80 of them

have never used it; SOP is not yet specifically related to tracking cybercrime perpetrators of VPN and TOR users; and many cases handled by BSSN are related to hate speech and provocation, especially those spread through social media.

The author summarizes the above results, that BSSN methods and strategies in dealing with cyber attacks include forming Gov-CSIRT and Pusopskamsinas; use Honeynet as an early detection system for cyber attacks; counterattacking perpetrators and coordinating with law enforcement.

The BSSN response step in dealing with terror threat attacks that enter the BSSN network is that the attack will activate the Honeypot sensor, then the danger signal is recorded in the Honeypot log. Dionaea in the Honeypot sensor will analyze the source of the attack so that the perpetrator's IP address will be tracked from the last path traveled and the timestamp. These results will be visualized on the Honeynet BSSN website, then carried out IP address tracking, network analysis used by the perpetrators to obtain the perpetrator's IP address.

Based on the author's analysis, cybercrime perpetrators who use VPN and TOR can be traced due to DNS and WebRTC leaks, detected TOR relay movements, and unencrypted TOR exit nodes.

To fill the limitations of the authority of BSSN in tracking cybercrime perpetrators, especially those who carry out attacks through social media accounts that use VPN and TOR, the author request and recommend BSSN about creating project profiles for each social media that is used by using information that can be extracted from the account profile.

The obstacles found in this research are procedural related, limited time in research, limitations of BSSN's human resources and BSSN policies related to data documentation and confidentiality. The recommendation that the author gives to BSSN is regarding the issuance of SOP for tracking cybercrime perpetrators who use VPN and TOR and SOP for profiling on social media accounts as well as the formulation of policies regarding the use of social media for investigations.

The conclusion of this study project profiling through social media accounts can help the process of tracking perpetrators of cybercrime VPN and TOR users in BSSN agency by continuing to coordinate with law enforcement officers.