DAFTAR ISI

Halaman

Halaman Sampul Depan i
Halaman Sampul Dalam ii
Halaman Prasyarat Gelar iii
Halaman Persetujuan iv
Halaman Penetapan Panitia Penguji v
Halaman Pernyataan vi
Halaman Ucapan Terima Kasih vii
Halaman Ringkasan x
Halaman *Summary* xii
Halaman Abstrak xiv
Halaman *Abstract* xv
DAFTAR ISI xvi
DAFTAR GAMBAR xviii
DAFTAR TABEL xx
DAFTAR LAMPIRAN xxi
DAFTAR SINGKATAN xxii

BAB 1 PENDAHULUAN
1.1. Latar Belakang 1
1.2. Rumusan Masalah 7
1.3. Tujuan Penelitian 7
1.3.1. Tujuan Umum 7
1.3.2. Tujuan Khusus 8
1.4. Manfaat Penelitian 8
1.4.1. Secara Akademis 8
1.4.2. Secara Praktis 8

BAB 2 TINJAUAN PUSTAKA
2.1. Kejahatan Siber (*Cyber Crime*) 9
2.2. *Virtual Private Network* (VPN) 20
2.3. *The Onion Router* (TOR) 25
2.4. Metode *Cyberprofiling* 36

BAB 3 KERANGKA KONSEPTUAL DAN HIPOTESIS PENELITIAN
3.1. Kerangka Konseptual Penelitian 52
3.2. Penjelasan Kerangka Konseptual 52
3.3. Hipotesis Penelitian 54

BAB 4 MATERI DAN METODE PENELITIAN
4.1. Jenis Penelitian dan Rancangan Penelitian 55
4.2. Populasi, Besar Sampel dan Teknik Pengambilan Sampel 56
4.3. Bahan Penelitian 58
4.4. Instrumen Penelitian 59
4.5. Lokasi dan Waktu Penelitian 59
4.6. Prosedur Pengambilan dan Pengumpulan Data 59
4.7. Bagan Kerangka Operasional 63
4.8. Analisis Data 63

BAB 5 ANALISIS HASIL PENELITIAN
5.1. Hasil Observasi 64
5.2. Hasil Wawancara dan Kuesioner 68

BAB 6 PEMBAHASAN
6.1. Prosedur dan Strategi Penanganan Serangan Siber 96
6.2. Penyebab Pengguna VPN dan TOR Terlacak 110
6.3. *Project Profiling* pada Akun Media Sosial 119
6.4. Analisis Hambatan dan Rekomendasi 131

BAB 7 KESIMPULAN DAN SARAN
7.1. Kesimpulan 136
7.2. Saran 137

DAFTAR PUSTAKA 139
LAMPIRAN 144

DAFTAR GAMBAR

No. Uraian Gambar Hal.

Gambar 2.1 Jenis kejahatan siber (tipe, motif dan alat serta teknologi yang digunakan)....12
Gambar 2.2 Protokol investigasi kejahatan siber menurut Yong Dal Shin 19
Gambar 2.3 Koneksi VPN membentuk sebuah "terowongan" (*tunnel*) melalui jaringan publik yaitu internet 22
Gambar 2.4 Penggunaan *Wireshark* pada Jaringan tanpa VPN 24
Gambar 2.5 Penggunaan *Wireshark* pada Jaringan dengan VPN....24
Gambar 2.6 Ilustrasi pengiriman pesan menggunakan TOR.... 28
Gambar 2.7 Serangan *man-in-the-middle* memaksa klien untuk memulai sesi dengan peretas alih-alih tujuan....34
Gambar 2.8 Pernyataan kebijakan privasi layanan *Gmail* 47
Gambar 2.9 Pernyataan kebijakan privasi layanan *Facebook*.... 47
Gambar 2.10 Pernyataan kebijakan privasi layanan *WhatsApp* 48
Gambar 2.11 Tampilan profil akun *Facebook* 49
Gambar 2.12 Tampilan profil akun *WhatsApp messenger*.... 50
Gambar 2.13 Tampilan profil pengirim dalam *Gmail* 50
Gambar 3.1 Kerangka konseptual penelitian 52
Gambar 4.1 Struktur organisasi BSSN. Lokasi penelitian ditandai dengan kotak biru 59
Gambar 4.2 *Project profiling* pada akun *Facebook*.... 61
Gambar 4.3 *Project profiling* pada akun *WhatsApp* 61
Gambar 4.4 *Project profiling* pada akun *E-mail*.... 62
Gambar 4.5 Bagan kerangka operasional 63
Gambar 5.1 Bagan mekanisme penanganan serangan siber....68
Gambar 5.2 Diagram lingkaran yang menunjukkan persentase pengetahuan responden masyarakat tentang VPN dan TOR 85
Gambar 5.3 Diagram lingkaran yang menunjukkan persentase ketertarikan responden masyarakat untuk mengetahui tentang VPN dan TOR.... 85
Gambar 5.4 Diagram lingkaran yang menunjukkan persentase pengalaman pernah atau tidak responden masyarakat menggunakan layanan VPN dan TOR 87
Gambar 5.5 Diagram lingkaran yang menunjukkan persentase ketertarikan responden masyarakat untuk mencoba menggunakan layanan VPN dan TOR 88

Gambar 5.6 Pelacakan alamat IP pengirim sebenarnya menggunakan IP *tracker*, tampak alamat IP sebenarnya serta ISP pengirim, dan lokasi pengirim ditunjukkan pada peta di atas..... 94
Gambar 6.1 Skema prosedur penanganan serangan siber..... 104
Gambar 6.2 Tampilan visualisasi hasil sensor *Honeypot* pada situs web *honeynet.bssn.go.id*..... 106
Gambar 6.3 Ilustrasi kebocoran DNS..... 112
Gambar 6.4 Pendeteksian adanya *middlebox* menggunakan aplikasi OONI Probe pada 2 (dua) *provider* seluler..... 117
Gambar 6.5 Tidak terdeteksi adanya *middlebox* menggunakan aplikasi OONI Probe pada *provider* seluler tersebut..... 117
Gambar 6.6 Tampilan *website fingerprinting* dalam *Onion circuit* yang juga menunjukkan alamat IP pengguna (1)..... 118
Gambar 6.7 Tampilan *website fingerprinting* dalam *Onion circuit* yang juga menunjukkan alamat IP pengguna (2)..... 119
Gambar 6.8 *Project profiling* pada akun *Facebook*. Yang ditandai dengan kotak hijau adalah langkah yang dapat dilakukan BSSN, sedangkan kotak biru adalah alternatif metode yang penulis rekomendasikan untuk *profiling* pelaku..... 122
Gambar 6.9 *Project profiling* pada akun *WhatsApp*. Yang ditandai dengan kotak hijau adalah langkah yang dapat dilakukan BSSN, sedangkan kotak biru adalah alternatif metode yang penulis rekomendasikan untuk *profiling* pelaku..... 124
Gambar 6.10 Informasi akun pengguna *WhatsApp* berisi nomor telepon seluler, alamat IP dan perangkat yang digunakan..... 125
Gambar 6.11 Informasi akun pengguna *WhatsApp* juga dapat menunjukkan daftar kontak dan grup yang terhubung dengan akun tersebut 125
Gambar 6.12 Informasi akun pengguna *WhatsApp* menunjukkan perangkat dan jaringan ISP yang digunakan..... 126
Gambar 6.13 Bukti digital rekam jejak riwayat chat melalui aplikasi *WhatsApp* yang tersimpan dalam *file database WhatsApp* dalam *smartphone*. Tampak *file* tersimpan dalam format terenkripsi..... 127
Gambar 6.14 *Project profiling* pada akun *e-mail*. Yang ditandai dengan kotak hijau adalah langkah yang dapat dilakukan BSSN, sedangkan kotak biru adalah alternatif metode yang penulis rekomendasikan untuk *profiling* pelaku..... 129

DAFTAR TABEL

Tabel 5.1 Daftar regulasi BSSN yang diobservasi 64

DAFTAR LAMPIRAN

Lampiran 1 Pedoman Wawancara dan Lembar Observasi..... 144
Lampiran 2 Contoh Kuesioner 163
Lampiran 3 Dokumentasi 178
Lampiran 4 Surat Ijin Penelitian..... 181
Lampiran 5 Form Permohonan Informasi pada BSSN 182
Lampiran 6 Peta Lokasi Penelitian..... 183

DAFTAR SINGKATAN

ACPO	= *The Association of Chief Police Officers*
API	= *Application Programming Interface*
APJII	= Asosiasi Penyelenggara Jasa Internet Indonesia
APT	= *Advanced Persistent Threat*
Aptika	= Aplikasi dan Informatika
AS	= Amerika Serikat
ATM	= *Asynchronous Transfer Mode*
BIN	= Badan Intelijen Negara
BSSN	= Badan Siber dan Sandi Negara
CERT	= *Computer Emergency Response Team*
CIPE	= *Cryptographic IP Encapsulation*
DDoS	= *Distributed Denial of Service*
Dittipidsiber	= Direktorat Tindak Pidana Siber
DPI	= *Deep Packet Inspection*
DNS	= *Domain Name System*
DoS	= *Denial of Service attack*
FBI	= *Federal Bureau of Investigation*
Gov-CSIRT	= *Government-Computer Security Incident Response Team*
GRE	= *Generic Routing Encapsulation*
HTML	= *Hypertext Markup Language*
HTTPS	= *Hypertext Transfer Protocol Secure*
IAFIS	= *Integrated Automated Fingerprint Identification System*
ID-SIRTII	= Indonesia *Security Incident Response Team on Internet Infrastucture*
IHP	= Indonesia *Honeynet Project*
IKE	= *Internet Key Exchang*
IP	= *Internet Protocol*
ISP	= *Internet Service Provider*
IPS	= *Interstate Photo System*
IPSec	= *Internet Protocol Security*
JSON	= *JavaScript Object Notation*
Juknis	= Petunjuk Teknis
Kemkominfo	= Kementerian Komunikasi dan Informatika
KPK	= Komisi Pemberantasan Korupsi
KTP	= Kartu Tanda Penduduk
L2F	= *Layer 2 Forwarding*
L2TP	= *Layer 2 Tunneling Protocol*
LAN	= *Local Area Network*
Lemsaneg	= Lembaga Sandi Negara
MAC	= *Media Access Control*

NGI = *Next Generation Identification*
NIK = Nomor Induk Kependudukan
Perpres = Peraturan Presiden
PETs = *Privacy Enhancing Technologies*
PPTP = *Point to Point Tunneling Protocol*
Polri = Kepolisian Republik Indonesia
Pusopskamsinas = Pusat Operasi Keamanan Siber Nasional
RUU KKS = Rancangan Undang-Undang Keamanan dan Ketahanan Siber
SARA = Suku, Agama, Ras dan Antar golongan
SDM = Sumber Daya Manusia
SME = *Subject Matter Expert*
SOC = *Security Operation Center*
SOP = Standar Operasional Prosedur
SSL = *Secure Socket Layer*
STSN = Sekolah Tinggi Sandi Negara
TIK = Teknologi Informasi dan Komunikasi
TKP = Tempat Kejadian Perkara
TLS = *Transport Layer Security*
TOR = *The Onion Router*
ULA = *Unique Local Address*
URL = *Uniform Resource Locator*
UU ITE = Undang-Undang Informasi dan Transaksi Elektronik
VPN = *Virtual Private Network*
WebRTC = *Web Real Time Communication*