BAB I
PENDAHULUAN

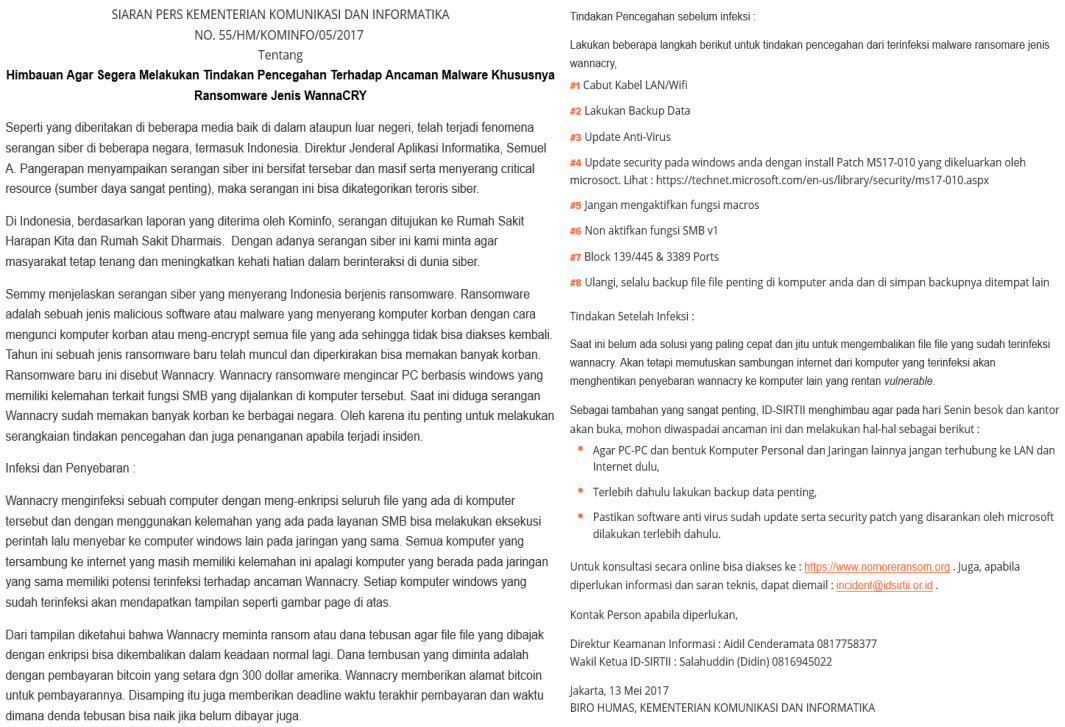
1.1 Latar belakang

Kemudahan yang dirasakan beriringan dengan berkembangnya zaman, membuat setiap manusia juga dimudahkan dalam setiap urusannya. Kemajuan teknologi tidak dipungkiri selalu menjadi kebutuhan yang berdampingan dalam kegiatan setiap manusia pada kesehariannya. Teknologi berkembang pada setiap bidang, salah satunya yaitu dalam media penyimpanan informasi, suatu informasi yang kita miliki kini bisa di simpan (*save)* dalam bentuk digital. Penyimpanan informasi atau data yang kita miliki dapat dimuat dalam suatu dokumen (*file)* pada suatu perangkat keras (*hardware)* yang biasa disebut sebagai komputer. Namun terkadang kemudahan tersebut dapat dimanfaatkan oleh beberapa pihak yang tidak bertanggungjawab dan dijadikan suatu keuntungan individu atas pihak yang dirugikan.

Terkait dengan kasus yang marak terjadi pada beberapa bulan lalu tepatnya pada 13 Mei 2017, yaitu fenomena serangan siber yang menyerang *critical resource* (sumber daya sangat penting). Serangan siber ini merupakan jenis Ransomware, Ransomware adalah sebuah jenis *malicious software* atau *malware* yang menyerang komputer korban dengan cara melakukan enkripsi pada semua dokumen yang ada sehingga tidak bisa diakses kembali. virus ini disebut sebagai Ransomware Wannacry, Wannacry mengincar PC berbasis windows yang memiliki kelemahan terkait fungsi SMB (*Server Message Block*) yang dijalankan di komputer tersebut. (sumber: https://kominfo.go.id/content/detail/9636/siaran-pers-no-55hmkominfo052017-tentang-himbauan-agar-segera-melakukan-tindakan-pencegahan-terhadap-ancaman-malware-khususnya-ransomware-jenis-wannacry/0/siaran_pers di akses pada 1 November 2017)

Wannacry menginfeksi sebuah komputer dengan mengenkripsi seluruh dokumen yang ada di komputer tersebut dan dengan menggunakan kelemahan yang ada pada layanan SMB bisa melakukan eksekusi perintah lalu menyebar ke komputer windows lain pada jaringan yang sama. Semua komputer yang tersambung ke internet yang masih memiliki kelemahan ini apalagi komputer yang berada pada

jaringan yang sama memiliki potensi terinfeksi terhadap ancaman Wannacry. Wannacry meminta *ransom* atau dana tebusan agar dokumen yang dibajak dengan enkripsi bisa dikembalikan dalam keadaan normal lagi. Dana tembusan yang diminta adalah dengan pembayaran *bitcoin* yang setara dengan 300 dollar Amerika. Wannacry memberikan alamat *bitcoin* untuk pembayarannya. Disamping itu juga memberikan batas waktu terakhir pembayaran dan waktu dimana denda tebusan bisa naik jika belum dibayar juga



SIARAN PERS KEMENTERIAN KOMUNIKASI DAN INFORMATIKA
NO. 55/HM/KOMINFO/05/2017
Tentang
Himbauan Agar Segera Melakukan Tindakan Pencegahan Terhadap Ancaman Malware Khususnya Ransomware Jenis WannaCRY

Seperti yang diberitakan di beberapa media baik di dalam ataupun luar negeri, telah terjadi fenomena serangan siber di beberapa negara, termasuk Indonesia. Direktur Jenderal Aplikasi Informatika, Semuel A. Pangerapan menyampaikan serangan siber ini bersifat tersebar dan masif serta menyerang critical resource (sumber daya sangat penting), maka serangan ini bisa dikategorikan teroris siber.

Di Indonesia, berdasarkan laporan yang diterima oleh Kominfo, serangan ditujukan ke Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais. Dengan adanya serangan siber ini kami minta agar masyarakat tetap tenang dan meningkatkan kehati hatian dalam berinteraksi di dunia siber.

Semmy menjelaskan serangan siber yang menyerang Indonesia berjenis ransomware. Ransomware adalah sebuah jenis malicious software atau malware yang menyerang komputer korban dengan cara mengunci komputer korban atau meng-encrypt semua file yang ada sehingga tidak bisa diakses kembali. Tahun ini sebuah jenis ransomware baru telah muncul dan diperkirakan bisa memakan banyak korban. Ransomware baru ini disebut Wannacry. Wannacry ransomware mengincar PC berbasis windows yang memiliki kelemahan terkait fungsi SMB yang dijalankan di komputer tersebut. Saat ini diduga serangan Wannacry sudah memakan banyak korban ke berbagai negara. Oleh karena itu penting untuk melakukan serangkaian tindakan pencegahan dan juga penanganan apabila terjadi insiden.

Infeksi dan Penyebaran :

Wannacry menginfeksi sebuah computer dengan meng-enkripsi seluruh file yang ada di komputer tersebut dan dengan menggunakan kelemahan yang ada pada layanan SMB bisa melakukan eksekusi perintah lalu menyebar ke computer windows lain pada jaringan yang sama. Semua komputer yang tersambung ke internet yang masih memiliki kelemahan ini apalagi komputer yang berada pada jaringan yang sama memiliki potensi terinfeksi terhadap ancaman Wannacry. Setiap komputer windows yang sudah terinfeksi akan mendapatkan tampilan seperti gambar page di atas.

Dari tampilan diketahui bahwa Wannacry meminta ransom atau dana tebusan agar file file yang dibajak dengan enkripsi bisa dikembalikan dalam keadaan normal lagi. Dana tembusan yang diminta adalah dengan pembayaran bitcoin yang setara dgn 300 dollar amerika. Wannacry memberikan alamat bitcoin untuk pembayarannya. Disamping itu juga memberikan deadline waktu terakhir pembayaran dan waktu dimana denda tebusan bisa naik jika belum dibayar juga.

Tindakan Pencegahan sebelum infeksi :

Lakukan beberapa langkah berikut untuk tindakan pencegahan dari terinfeksi malware ransomare jenis wannacry,

#1 Cabut Kabel LAN/Wifi

#2 Lakukan Backup Data

#3 Update Anti-Virus

#4 Update security pada windows anda dengan install Patch MS17-010 yang dikeluarkan oleh microsoct. Lihat : https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

#5 Jangan mengaktifkan fungsi macros

#6 Non aktifkan fungsi SMB v1

#7 Block 139/445 & 3389 Ports

#8 Ulangi, selalu backup file file penting di komputer anda dan di simpan backupnya ditempat lain

Tindakan Setelah Infeksi :

Saat ini belum ada solusi yang paling cepat dan jitu untuk mengembalikan file file yang sudah terinfeksi wannacry. Akan tetapi memutuskan sambungan internet dari komputer yang terinfeksi akan menghentikan penyebaran wannacry ke komputer lain yang rentan *vulnerable*.

Sebagai tambahan yang sangat penting, ID-SIRTII menghimbau agar pada hari Senin besok dan kantor akan buka, mohon diwaspadai ancaman ini dan melakukan hal-hal sebagai berikut :

- Agar PC-PC dan bentuk Komputer Personal dan Jaringan lainnya jangan terhubung ke LAN dan Internet dulu,
- Terlebih dahulu lakukan backup data penting,
- Pastikan software anti virus sudah update serta security patch yang disarankan oleh microsoft dilakukan terlebih dahulu.

Untuk konsultasi secara online bisa diakses ke : https://www.nomoreransom.org . Juga, apabila diperlukan informasi dan saran teknis, dapat diemail : incident@idsirtii.or.id .

Kontak Person apabila diperlukan,

Direktur Keamanan Informasi : Aidil Cenderamata 0817758377
Wakil Ketua ID-SIRTII : Salahuddin (Didin) 0816945022

Jakarta, 13 Mei 2017
BIRO HUMAS, KEMENTERIAN KOMUNIKASI DAN INFORMATIKA

Gambar 1.1 Press Release Kemkominfo

Sumber : kemkominfo.go.id

Penyebaran *malware* berjenis Ransomware Wannacry ini serentak menyebar dalam hitungan 24 jam diseluruh dunia tak terkecuali Indonesia, 45000 instalasi atau komputer terpapar *malware* ini sedangkan Petya itu berbeda, Petya hanya mampu menyebar pada 11000 unit komputer. Tim IDSIRTII mendapatkan info bahwa beberapa bagian Negara eropa dan inggris raya telah terkena *malware* berjenis Ransomware Wannacry yang informasinya telah di confirm kepada member CERT (*Computer Emergency Response Team)* lainnya seperti *APCERT (Asia pacific Computer Emergency Response Team), OIC-CERT Organisation of Islamic*

Cooperation – Computer Emergency Response Team, Forum of Incident Response and Security Team. Pada tanggal 12 Mei 2017 juga telah terdeteksi bahwa *malware* berjenis Ransomware Wannacry ini memasuki wilayah Negara Indonesia yang mengarah kepada rumah sakit Dharmais Jakarta, yang diketahui oleh tim ID-SIRTII melalui layar pemantau terlihat melalui no IP. Kemudian tim Kemkominfo mengkomunikasikan lebih lanjut pada grup *chat*, email, dan juga telefon pada internal Kemkominfo hingga diputuskan untuk mengeluarkan peringatan dini pada tanggal 13 Mei 2017 yang di sampaikan melalui siaran pers no. 55/HM/KOMINFO/05/2017 yang dituliskan oleh Biro Humas pada situs resmi Kemkominfo yang berisi tentang himbauan serta langkah tindakan pencegahan atas *malware* Ransomware Wannacry ini. Kemkominfo menerbitkan *press release* ini dalam rangka memberitahukan informasi umum dan juga penerangan bagi masyarakat tentang Ransomware Wannacry.

Setelah mengeluarkan peringatan dini dengan siaran pers pertama, pada hari Minggu siang 14 Mei 2017 Kemkominfo memutuskan untuk melakukan konferensi pers di Bakoel Koffie Cikini, Jakarta dengan rekan-rekan media. Konferensi pers ini ikut dihadiri oleh Menteri Komunikasi dan Informatika dan beberapa pemangku kepentingan lainnya serta Biro Humas juga turut mengundang organisasi-organisasi swasta ataupun personal yang mengerti dalam hal ini. Setelah mengadakan konferensi pers pada Minggu siang 14 Mei 2017, Kemkominfo mengadakan rapat internal kembali di gedung Kemkominfo lantai 2 di Jalan Medan Merdeka Jakarta, yang salah satu isi dari rapat yaitu berupa meminta semua operator untuk mengirim pesan yang dapat dihubungkan dengan situs kominfo dan akan menampilkan panduan atas Ransomware Wannacry dan juga infografis antisipasi Ransomware Wannacry.

Gambar 1.2 Infografis Antisipasi Ransomware Wannacry

Sumber: kemkominfo.go.id

Selain itu humas dari Kemkominfo juga membuat infografis dan juga konten youtube, dalam rangka memudahkan masyarakat untuk memahami pesan dengan cara penyampaian yang lebih sederhana. Penyampaian ini juga disebarkan melalui situs resmi Kemkominfo dan media sosial *twitter official* Kemkominfo. Isi dari infografis ini merupakan tips sederhana dalam mengatasi serangan *malware* Ransomware Wannacry, terdapat tahap awal hidupkan komputer/*server* terlebih dahulu matikan *hotspot/wifi* dan cabut koneksi kabel LAN/internet, hingga tahap akhir segera pindahkan data ke sistem operasi non windows (linux, mac) atau lakukan *back up/copy* semua data ke *media storage* terpisah. Disertakan juga kontak orang-orang pemangku kepentingan atas kasus ini.

Kemudian humas dari Kemkominfo juga membuat *SMS blast* yang disebarkan melalui operator-operator yang berisi edukasi dan informasi. Dalam penyebaran *SMS blast* diharapkan informasi ini menyebar secara menyeluruh kepada tiap-tiap masyarakat. Dikarenakan penyebaran *SMS blast* ini dilakukan pada hari libur kantor, yaitu pihak Kemkominfo meminta kepada setiap operator untuk blast *SMS* ini mulai hari Minggu, maka dari itu ketika mulai beraktifas normal di hari Senin diharapkan dapat langsung melakukan isolasi pada setiap unit komputer.

Gambar 1.3 *SMS Blast* Kemkominfo

Sumber: Dokumen Pribadi & kemkomingo.go.id

Setelah Kemkominfo menerbitkan *press release* dan juga melakukan penyebaran informasi melalui berbagai media, masyarakat pun mulai resah dalam menghadapi penyebaran *malware* Ransomware Wannacry, mereka takut komputer pribadi mereka juga terkena virus Wannacry yang sedang menyebar di dunia, sehingga muncul banyak tanggapan masyarakat atas penyebaran informasi yang di terbitkan oleh Kemkominfo ini, salah satunya yaitu tanggapan yang diambil melalui media sosial *twitter*. Respon masyarakat secara langsung ditanggapi oleh tim humas Kemkominfo, tim ID-SIRTII (*Indonesia Security Incident Response Team on Internet Infrastructure)* serta beberapa pemangku penting lainnya yang ditunjuk sebagai *spokeperson* seperti Direktur Aptika dan juga Direktur Keamanan Dan Informasi. Bisa dibilang ID-SIRTII merupakan sebagai dinding pertahanan pertama dalam menghadapi serangan di dunia maya, ID-SIRTII juga dibanjiri dengan berbagai pertanyaan melalui layanan informasi publik dalam bentuk layanan telefon yang dicantumkan dalam *press release* sejak 13 Mei 2017.

Gambar 1.4 Pertanyaan dan Aduan Wannacry

Sumber: twitter.com/kemkominfo

Jangka waktu dalam pemulihan penyebaran *malware* berjenis Ransomware Wannacry ini cukup terbilang singkat dan hanya memakan sedikit korban yang hanya dapat dihitung jari. Dengan penyebarannya di 150 negara dalam waktu 24 jam, yang mencapai angka 45000 unit komputer yang telah terkena virus *malware* berjenis Ransomware ini Indonesia tercatat hanya terkena di 9 perusahaan saja hingga saat ini.

> *"Serangan Ransomware ini menjadi isu global, sehingga penyelesaiannya juga secara internasional. Indonesia bukan menjadi negara terbesar yang terkena serangan"* Rudiantara, Menteri Komunikasi dan Informatika melalui konferensi pers yang dilakukan di Bakoel Koffie, Cikini, Jakarta pada hari Minggu 14 mei 2017 *(*sumber: https://www.kominfo.go.id/content/detail/9638/menkominfo-perlu-kecepatan-tangani-serangan-Ransomware-Wannacry/0/berita_satker?utm_source=dlvr.it&utm_medium=twitter diakses pada tanggal 28 Desember 2017)

Keberhasilan Kemkominfo dalam melakukan manajemen krisis ini dapat dikatakan berhasil, dikarenakan efek yang ditimbulkan yaitu berupa laporan perusahaan yang melapor hanya terdapat 9 perusahaan saja. Pada tanggal 17 Mei 2017 Menkominfo telah mengudarakan pernyataannya bahwa Indonesia telah aman dari Ransomware Wannacry, namun belum 100 persen (sumber:

youtube.com/cnnindonesia https://www.youtube.com/watch?v=iuPa9Uvti8k diakses pada tanggal 28 desember 2017)

Menurut Dimock dan Koenig (1987) dalam Ruslan (2012:342), mengatakan bahwa pada umumnya tugas-tugas pihak humas instansi atau lembaga pemerintahan, yaitu sebagai berikut.

1) Memberikan penerangan atau informasi kepada masyarakat tentang pelayanan masyarakat, kebijaksanaan serta tujuan yang akan dicapai oleh pemerintah dalam melaksanakan program kerja tersebut. Dalam hal ini Kemkominfo harus menjalankan tugasnya dalam menyebarkan informasi mengenai penyebaran Wannacry dan juga langkah-langkah antisipasi terkena virus *malware* Wannacry
2) Mampu untuk menanamkan keyakinan dan kepercayaan serta mengajak masyarakat dalam partisipasinya atau ikut serta pelaksanaan program pembangunan di berbagai bidang, sosial, budaya, ekonomi, politik serta menjaga stabilitas dan keamanan nasional. Kemkominfo memberikan penyuluhan dengan mengatasi penyebaran informasi-informasi resmi serta menuliskan 'jangan panik' dengan menambahkan informasi mendetail yang meyakinkan
3) Kejujuran dalam pelayanan dan pengabdian dari aparatur pemerintah yang bersangkutan perlu dipelihara atau dipertahankan dalam melaksanakan tugas serta kewajibannya masing-masing. Kemkominfo bertanggungjawab penuh atas kasus ini karena melibatkan kepentingan orang banyak

Dalam kasus Ransomware Wannacry ini menyangkut krisis dengan faktor *safety and security issues* di indonesia, bagaimana peran lembaga pemerintah menghadapi berbagai strategi yang terapkan dalam penanganan terkait dengan kasus tersebut. Kementerian Komunikasi dan Informatika bertugas bertanggungjawab atas kasus penyebaran Ransomware di Indonesia. Pada kasus ini keamanan informasi pada setiap perusahaan maupun individu sedang terancam, dimana data yang tersebut menyangkut kepentingan orang banyak. Wannacry ini menyerang instansi penting seperti rumah sakit dan perbankan yang aktif 24 jam tersambung internet dan juga memiliki keamanan data rendah pada sistem kemanan yang dimiliki pada unit-unit komputernya, penyerangan *malware* jenis Ransomware Wannacry ini menyerang sistem operasi berstandar rendah dengan keamanan yang rendah juga. Seperti yang

sudah diumumkan oleh Kemkominfo melalui konferensi pers bahwa virus ini menyerang pengguna windows dengan *operating system* dibawah 2008 dan lemahnya anti virus yang dimiliki.

Pada penelitian ini peneliti menemukan urgensi berupa penyebaran yang terjadi harus ditangani dengan tepat dan cepat, seperti pada kasus penyebaran Ransomware Wannacry di London,

> "*Masalah muncul Jumat pagi ketika rumah sakit-rumah sakit di Inggris mendapat serangan siber skala besar yang mengakibatkan dibatalkannya pengerahan tenaga kesehatan dan pengalihan ambulans. Para pekerja kesehatan kemudian melapor bahwa akses mereka terkunci dan mereka menerima pesan untuk membayar ransum jika ingin mengembalikan akses akun yang dibajak tadi. Setidaknya ada 16 organisasi yang bekerja sama dengan NHS.*" (sumber: https://news.detik.com/internasional/d-3499719/komputer-rs-di-inggris-kena-virus-yang-batalkan-pengiriman-ambulans diakses pada 6 Februari 2018).

Pada kutipan berita tersebut dapat disimpulkan betapa bahayanya apabila penyebaran harus terjadi pada skala besar sehingga dibutukan ketepatan dalam melakukan tindakan dan menekan penyebaran virus. Selain itu peneliti juga ingin mengetahui permasalahan yang dialami oleh perusahaan dan negara dalam menyampaikan pesan yaitu terjadinya perbedaan kognisi antara sumber dan *receiver* sehingga dibutuhkannya seorang PR dalam menangani kasus ini.

Peneliti ingin melihat bagaimana peran perusahaan non-komersial yaitu organinsasi pemerintahan Kementerian Komunikasi dan Informatika dalam menangani kasus yang terjadi, maka dari itu peneliti mengambil judul **"MANAJEMEN KRISIS KEMENTERIAN KOMUNIKASI DAN INFORMATIKA (STUDI KASUS: PENYEBARAN RANSOMEWARE WANNACRY DI INDONESIA"**

peneliti ingin mengetahui bagaimana humas serta jajaran internal yang terkait dalam perusahaan non-komersial pemerintah bertugas dalam mengkomunikasikan bagaimana krisis komunikasi yang terjadi kepada masyarakat umum serta strategi manajemen yang diterapkan dengan teoritis yang ada.

1.2 Fokus Penelitian

Dalam penelitian, ini peneliti perlu memfokuskan batasan-batasan masalah yang diharapkan mampu membahas sesuai dengan tujuan peneliti maka dari itu peneliti membagi fokus penelitian atas:

1) Bagaimana pemetaan dan penanggulangan krisis mulai dari faktor hingga tahapan-tahapan krisis yang dilalui oleh Kemkominfo?
2) Bagaimana penerapan manajemen krisis mulai dari langkah-langkah yang dipilih hingga penyelesaian yang terjadi dapat dipecahkan oleh Kemkominfo?

1.3 Identifikasi Masalah

1) Mengetahui bagaimana penjelasan krisis yang terjadi akibat faktor *safety and security issues* oleh Kemkominfo.
2) Tahapan-tahapan krisis apa saja yang dilalui oleh Kemkominfo dalam penyebaran *malware* Ransomware Wannacry oleh Kemkominfo.
3) Langkah-langkah apa saja yang digunakan dalam manajemen krisis oleh Kemkominfo.
4) Penyelesaian krisis dalam manajemen krisis sampai terpecahkan oleh Kemkominfo.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini yaitu, peneliti mengharapkan dapat mengetahui dari apa yang difokuskan dalam fokus penelitian

1) Mengetahui bagaimana pemetaan krisis mulai dari faktor hingga tahapan-tahapan krisis yang dilalui oleh Kemkominfo.
2) Mengetahui bagaimana penerapan manajemen krisis mulai dari langkah-langkah yang dipilih hingga penyelesaian yang terjadi dapat dipecahkan oleh Kemkominfo.

1.5 Kegunaan Penelitian

1) Kegunaan Praktis

Peneliti mengharapkan, penelitian ini dapat bermanfaat bagi Kementerian Komunikasi dan Informatika apabila kedepannya mendapatkan kasus krisis komunikasi serupa dan dapat dimanfaatkan dalam dunia praktis.

2) Kegunaan Teoritis

Peneliti mengharapkan dengan penelitian ini dapat bermanfaat bagi perkembangan ilmu pengetahuan dan akademis kedepannya.

1.6 Waktu dan Periode Penelitian

Penelitian ini akan dilakukan di kantor Kementerian Komunikasi dan Informatika, Jakarta Pusat, dimulai dari bulan September 2017. Rinciannya dapat dilihat pada tabel berikut

Tabel 1.1 Waktu dan Periode Penelitian

Tahapan	2017				2018
	Sept	Okt	Nov	Des	Jan
Menentukan judul					
Mancari informasi awal penelitian					
Penyusunan proposal					
Desk evaluation					
Pengumpulan dan pengolahan data					
Penyusunan skripsi					