**MAKALAH ETIKA PROFESI TEKNOLOGI INFORMASI KOMUNIKASI**

**DISTRIBUTED DENIAL OF SERVICES ATTACK / DDOS ATTACK**

****

Diajukan untuk memenuhi nilai UAS pada mata kuliah EPTIK

**Muhammad Husein 1214**

**Fikri Hidayat 1214**

**Rahmad Bannie Adji 1214**

**Arif Trian Nugroho 12146005**

**Andro julio 1214**

**Program Studi Manajemen Informatika**

**AMIK BSI Jakarta**

**Jakarta**

**2017**

**KATA PENGANTAR**

Puji syukur Alhamdulillah, penulis panjatkan kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-nya sehingga pada akhirnya penulis dapat menyelesaikan tugas makalah ini dengan baik, adapun judul penulisan makalah yang penulis ambil adalah sebagai berikut: berjudul **“Makalah Etika Profesi Teknologi Informasi Komunikasi Distributed Denial Of Services Attack / DDOS Attack”.**

Tujuan penulisan makalah ini dibuat untuk memenuhi nilai UAS mata kuliah Etika Profesi Teknologi Informasi dan Komunikasi (EPTIK) pada Program Diploma III ( D.III ) AMIK BSI. Sebagai bahan penulisan diambil berdasarkan hasil analisa, dan beberapa sumber literatur yang mengandung penulisan ini, penulis menyadari bahwa tanpa bimbingan dan dorongan dari semua pihak, maka penulisan makalah ini tidak berjalan lancar.

Akhir kata semoga makalah ini dapat berguna bagi penulis khususnya bagi pembaca. Penulis menyadari bahwa penulisan makalah ini masih jauh sekali dan belum sempurna, untuk itu penulis mohon kritik dan saran yang bersifat membangun demi kesempurnaan penulis dimasa akan datang.

Jakarta, Mei 2017

Penulis

**DAFTAR ISI**

Lembar Judul i

Kata Pengantar ii

Daftar Isi iii

Daftar Lampiran iv

**BAB I PENDAHULUAN**

* 1. Umum 1
  2. Maksud dan Tujuan 1
  3. Metode Penelitian 2
  4. Ruang Lingkup 2
  5. Sistematika Penulisan 3

**BAB II LANDASAN TEORI**

* + 1. Cyber Crime 4
    2. Cyber Law 5
    3. DDOS Attack 8

**BAB III PEMBAHASAN**

* + 1. Studi Kasus 13
    2. Analisa Kasus 13
  1. Analisa Cyber Law 21

**BAB IV PENUTUP**

* + 1. Kesimpulan 24

**DAFTAR PUSTAKA**

**LAMPIRAN-LAMPIRAN**

**DAFTAR LAMPIRAN**

Lampiran A.1 Lembar Penilaian 26

Lampiran B.1 Capture Blog 27

Lampiran C.1 Curiculum Vitae 30

**BAB I**

**PENDAHULUAN**

* 1. **Umum**

Banyaknya penyedia internet dan semakin terjangkaunya biaya akses internet membuat banyak orang mulai mengenal internet dan menggunakannya. Hal tersebut membuat para cyber crime melakukan aksi penyerangan komputer / server dengan memanfaatkan kesadaran masyarakat dalam hal ini pengguna komputer dan internet yang masih kurang mengerti akan dampak negatif dari internet serta ke tidak sempurnaan kebijakan-kebijakan pemerintah dalam hal tersebut.

Oleh sebab itu, penulis membuat sebuah studi kasus yang sekiranya dapat membantu menganalisis kasus cybercrime berdasarkan Undang-Undang ITE tahun 2016 dan penulis menuangkan ke dalam sebuah makalah yang berjudul **“Makalah Etika Profesi Teknologi Informasi Komunikasi Distributed Denial Of Services Attack / DDOS Attack” .**

* 1. **Maksud dan Tujuan**

Adapun maksud dari studi kasus yang dilaksanakan penulis adalah sebagai berikut:

1. Menganalisa kasus DDOS Attack.
2. Menganalisa Cyber Law yang diterapkan berdasarkan Undang-Undang ITE tahun 2016.

Sedangkan Tujuan pembuatan makalah ini antara lain:

1. Memenuhi mata kuliah Etika Profesi Teknoligi Informasi Komunikasi (EPTIK) semester enam jurusan manajemen informatika AMIK BSI.
2. Sebagai Penilaian Tugas Pengganti UAS Etika Profesi Teknoligi Informasi Komunikasi (EPTIK) semester enam jurusan manajemen informatika AMIK BSI.

**1.3 Metode Penelitian**

Adapun metode yang digunakan pada saat analisa kasus sebagai berikut :

1. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan oleh penulis dalam melakukan pengumpulan data untuk pembuatan makalah, yaitu :

1. Studi Pustaka

Untuk melengkapi tugas makalah ini penulis mengambil beberapa referensi dari buku-buku dan link dari website yang berkaitan dengan kasus.

**1.4 Ruang Lingkup**

Dalam penulisan makalah ini penulis menerangkan ruang lingkup mencangkup masalah kejahatan di dunia teknologi komputer, khusus nya dalam kejahatan DDOS attack.

**1.5 Sistematika Penulisan**

Sistematika penulisan makalah ini terdiri dari empat bab, yang masing-masing memiliki penjelasan secara terperinci, berikut gambaran sistematika studi kasus penyerangan virus stuxnet, yaitu :

BAB I PENDAHULUAN

Pada bab ini penulis menjelaskan latar belakang, maksud dan tujuan penulisan, metode penulisan dalam melakukan pengambilan data, ruang lingkup penulisan, dan sistematika penulisan secara keseluruhan.

BAB II LANDASAN TEORI

Pada bab ini kami menjelaskan konsep dasar sistem dan teori pendukung dalam penulisan makalah ini.

BAB III PEMBAHASAN

Pada bab ini penulis menjelaskan inti dari makalah yang dimulai dari analisa kasus, yang berisi tentang penjelasan kasus yang di analisa dan dilanjutkan menjelaskan inti dari bab ini yaitu penjabaran Cyber law.

BAB IV PENUTUP

Pada bab ini penulis memberikan kesimpulan dari studi kasus dan analisa kasus yang telah dilakukan.

**BAB II**

**LANDASAN TEORI**

* 1. **Cyber Crime**

Cybercrime adalah tidak criminal yang dilakkukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. Cybercrime merupakan kejahatan yang memanfaatkan perkembangan teknologi computer khusunya internet. Berikut adalah beberapa jenis cybercrime:

1. Jenis cyber crime berdasarkan Karakteristiknya:
   * + - 1. Cyberpiracy
         2. Cybertrespass
         3. Cybervandalism
2. Jenis Cyber crime berdasarkan aktivitasnya:
   * + 1. Illegal Contents (Konten Tidak Sah)
       2. Data Forgery (Pemalsuan Data)
       3. Cyber Spionase (Mata-mata)
       4. Data Theft (Mencuri Data)
       5. Misuse of devices (Menyalahgunakan Peralatan Komputer)
       6. Hacking dan Cracker
       7. DoS (Denial Of Service)
       8. Cybersquatting and Typosquatting
       9. Hijacking
       10. Cyber Terorism
       11. Unauthorized Access to Computer System and Service
       12. Ilegal Access (Akses Tanpa Ijin ke Sistem Komputer)
   1. **Cyber Law**

Cyber Law yaitu Hukum yang membatasi kejahatan cyber (kejahatan dunia maya melalui jaringan internet). Cyber Law diperlukan atas dasar dari hukum di berbagai negara yaitu "ruang dan waktu".

Sementara jaringan komputer dan internet telah mendobrak batas ruang dan waktu tersebut .Meskipun alat buktinya berbentuk virtual dan bersifat elektronik kegiatan cyber adalah kegiatan virtual yang berdampak nyata.

Cyberlaw bukanlah suatu keharusan, namun sudah merupakan kebutuhan untuk menghadapi kenyataan yang ada pada saat ini, yaitu adanya tindak kejahatan di internet atau yang di sebut dengan cybercrime

Cyberlaw adalah hukum yang digunakan di dunia cyber (dunia maya), yang umumnya diasosiasikan dengan Internet. Cyberlaw dibutuhkan karena dasar atau fondasi dari hukum di banyak negara adalah "ruang dan waktu". Sementara itu, Internet dan jaringan komputer mendobrak batas ruang dan waktu ini.

Cyber Law juga didefinisikan sebagai kumpulan peraturan perundang-undangan yang mengatur tentang berbagai aktivitas manusia di cyberspace (dengan memanfaatkan teknologi informasi). Cyber Law sendiri merupakan istilah yang berasal dari Cyberspace. Cyberspace berakar dari kata latin Kubernan yang artinya menguasai atau menjangkau. Karena ”cyberspace”-lah yang akan menjadi objek atau concern dari ”cyber law”.

Ruang lingkup dari Cyber Law meliputi hak cipta, merek dagang, fitnah/penistaan, hacking, virus, akses Ilegal, privasi, kewajiban pidana, isu prosedural (Yurisdiksi, Investigasi, Bukti, dll), kontrak elektronik, pornografi, perampokan, perlindungan konsumen dan lain-lain.

Perkembangan Cyber Law di Indonesia sendiri belum bisa dikatakan maju. Hal ini diakibatkan oleh belum meratanya pengguna internet di seluruh Indonesia. Berbeda dengan Amerika Serikat yang menggunakan telah internet untuk memfasilitasi seluruh aspek kehidupan mereka. Oleh karena itu, perkembangan hukum dunia maya di Amerika Serikat pun sudah sangat maju.

Landasan fundamental di dalam aspek yuridis yang mengatur lalu lintas internet sebagai hukum khusus, di mana terdapat komponen utama yang meng-cover persoalan yang ada di dalam dunai maya tersebut, yaitu :

1. Yurisdiksi hukum dan aspek-aspek terkait.

Komponen ini menganalisa dan menentukan keberlakuan hukum yang berlaku dan diterapkan di dalam dunia maya itu.

1. Landasan penggunaan internet sebagai sarana untuk melakukan kebebasan berpendapat yang berhubungan dengan tanggung jawab pihak yang menyampaikan, aspek accountability, tangung jawab dalam memberikan jasa online dan penyedia jasa internet (internet provider), serta tanggung jawab hukum bagi penyedia jasa pendidikan melalui jaringan internet.
2. Aspek hak milik intelektual di mana ada aspek tentang patent, merek dagang rahasia yang diterapkan, serta berlaku di dalam dunia cyber.
3. Aspek kerahasiaan yang dijamin oleh ketentuan hukum yang berlaku di masing-masing yurisdiksi negara asal dari pihak yang mempergunakan atau memanfaatkan dunia maya sebagai bagian dari sistem atau mekanisme jasa yang mereka lakukan.
4. Aspek hukum yang menjamin keamanan dari setiap pengguna dari internet.
5. Ketentuan hukum yang memformulasikan aspek kepemilikan didalam internet sebagai bagian dari pada nilai investasi yang dapat dihitung sesuai dengan prinisip-prinsip keuangan atau akuntansi.
6. Aspek hukum yang memberikan legalisasi atas internet sebagai bagian dari perdagangan atau bisnis usaha.

Berdasarkan faktor-faktor di atas, maka kita akan dapat melakukan penilaian untuk menjustifikasi sejauh mana perkembangan dari hukum yang mengatur sistem dan mekanisme internet di Indonesia. Walaupun belum dapat dikatakan merata, namun perkembangan internet di Indonesia mengalami percepatan yang sangat tinggi serta memiliki jumlah pelanggan atau pihak yang mempergunakan jaringan internet terus meningkat sejak paruh tahun 90'an.

Salah satu indikator untuk melihat bagaimana aplikasi hukum tentang internet diperlukan di Indonesia adalah dengan banyak perusahaan yang menjadi provider untuk pengguna jasa internet di Indonesia. Perusahaan-perusahaan yang memberikan jasa provider di Indonesian sadar atau tidak merupakan pihak yang berperanan sangat penting dalam memajukan perkembangan Cyber Law di Indonesia dimana fungsi-fungsi yang mereka lakukan seperti :

1. Perjanjian aplikasi rekening pelanggan internet.
2. Perjanjian pembuatan desain home page komersial.
3. Perjanjian reseller penempatan data-data di internet server.
4. Penawaran-penawaran penjualan produk-produk komersial melalui internet.
5. Pemberian informasi yang di-update setiap hari oleh home page komersial.
6. Pemberian pendapat atau polling online melalui internet.

Fungsi-fungsi di atas merupakan faktor dan tindakan yang dapat digolongkan sebagai tindakan yang berhubungan dengan aplikasi hukum tentang cyber di Indonesia. Oleh sebab itu ada baiknya di dalam perkembangan selanjutnya, setiap pemberi jasa atau pengguna internet dapat terjamin. Maka hukum tentang internet perlu dikembangkan serta dikaji sebagai sebuah hukum yang memiliki displin tersendiri di Indonesia.

* 1. ***Distributed Denial Of Service Attack* / DDOS *Attack***

*Distributed denial of services attack* atau lebih sering dibilang DDOS *attack* adalah jenis serangan yang dilakukan oleh attacker / hacker terhadap sebuah komputer atau server didalam jaringan internet dengan cara menghabiskan sumber daya (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat lagi menjalankan fungsinya dengan benar, sehingga secara tidak langsung mencegah pengguna lain untuk mengakses layanan dari komputer yang diserang tersebut.

Adapun jenis-jenis *distributed denial of server* atau DDOS *attack* adalah sebagai berikut :

1. Ping Of Death adalah Merupakan serangan klasik yang dulu sering digunakan. Serangan ini di dilancarkan dengan menggunakan utility ping pada sebuah sistem operasi. Ping biasanya digunakan untuk memeriksa keberadaan sebuah host atau alamat IP dari sebuah website. Data yang dikirimkan secara default adalah 32 bytes, namun pada kenyataannya program ini dapat mengirimkan sampai dengan 65 kilobytes data. Sekarang serangan seperti ini sudah tidak terlalu ampuh lagi, karena banyak sistem yang telah mengupdate patchnya dan menutup lubang-lubang tersebut. Ditambah semakin canggihnya teknologi dan semakin lebarnya bandwith yang tersedia, sehingga serangan ini tidak lagi menimbulkan dampak yang signifikan bagi sebuah sistem.
2. Syn flooding adalah Serangan yang dilakukan dengan cara memanfaatken kelemahan protokol pada saat terjadinya proses handshake(penyatuan). Saat dua buah komputer memutuskan untuk memulai melakukan komunikasi maka komputer pengirim (penyerang) akan mengirimkan syn, penerima (target) pun akan menjawab dengan mengirimkan syn ack kepada komputer pengirim. Seharusnya setelah menerima balasan syn ack dari penerima, pengirim mengirimkan ack kepada penerima untuk melakukan proses handshake. Namun pada kenyataannya, pengirim justru mengirimkan banyak paket syn kepada penerima yang mengakibatkan penerima harus terus menjawab permintaan dari pengirim. Alamat IP penyerang biasanya telah disembunyikan atau spoofed sehingga alamat yang dicatat oleh target adalah alamat yang salah. Penerima akan bingung untuk menjawab permintaan koneksi TCP yang baru karena masih menunggu banyaknya balasan ACK dari pengirim yang tidak diketahui tersebut. Disamping itu koneksi juga akan dibanjiri oleh permintaan syn yang dikirim oleh pengirim secara terus menerus. Serangan seperti ini menghambat penerima(server) memberikan pelayanan kepada user yang lain.
3. Remote controled attack adalah pada dasarnya adalah mengendalikan beberapa network lain untuk menyerang target. Penyerangan dengan tipe ini biasanya akan berdampak besar, karena biasanya server- server untuk menyerang mempunyai bandwith yang besar. Penyerang juga dengan leluasa dapat mengontrol bonekanya dan menyembunyikan diri dibalik server-server tersebut. Banyak tools yang dapat digunakan untuk melakukan serangan denga tipe ini. Umumnya tools tersebut mempunyai tipe Master dan client atau agent. Marster merupakan komputer master yang telah dikuasai oleh penyerang dan akan digunakan untuk memberikan perintah kepada para agent guna melancarkan serangan. Sedangkan client adalah komputer zombie yang telah berhasil dikuasai oleh penyerang, kemudian penyerang menanamkan aplikasi client yang siap menunggu perintah untuk menyerang target. Penyerang menggunakan dua buah master server yang digunakan untuk menyebarkan perintah kepada para zombie guna menyerang target. Setelah meremote server yang telah ditunjuk sebagai master, selanjutnya penyerang menggunakan server tersebut untuk mengirimpak perintah serangan kepada para zombie dalam hal ini adalah klien dari master server tersebut. Dengan menggunakan master server, penyerang dapat mengirimkan perintah ke banyak zombie asalkan telah adanya komunikasi antara zombie sabagi klien dan master server sebagai master. Setelah menerima perintah dari server, maka klien atau agen ini akan melakukan penyerangan sesuai yang diperintahkan oleh penyerang. Serangan yang dilakukan oleh banyak zombie inilah yang akan berakibat sangat fatal terhadap sistem target. Karena paket data yang dikirim tidak hanya berasal dari satu sumber, sehingga cukup sulit untuk melakukan pemblokiran alamat penyerang.
4. UDP (*User Datagram Protocol*) flood  adalah Serangan yang memanfaatkan protokol UDP dengan cara connectionless(mengurangi sambungan) untuk menyerang target. Karena sifatnya itulah UDP flood cukup mudah untuk dilakukan. Sejumlah paket data yang besar dikirimkan begitu saja kepada korban. Korban yang kaget dan tidak siap menerima serangan ini tentu akan bingung dan pada komputer server tersebut akan hang karena besarnya paket data yang diterima. Penyerang dapat menggunakan tehnik spoofed (penyamaran) untuk menyembunyikan identitasnya.
5. Smurf Attack adalah merupakan penyerangan dengan memanfaatkan ICMP (*Internet Control Message Protocol*) echo request yang sering digunakan pada saat broadcast (menyiarkan) identitas kepada broacast address dalam sebuah network. Saat melakukan broadcast pada broadcast address maka semua komputer yang terkoneksi kedalam jaringan akan ikut menjawab request tersebut. Hal ini tentu saja akan memperlambat trafik di jaringan karena komputer–komputer yang tidak ditanya turut memberikan request tersebut. Hal ini tentu akan berdampak lebih besar bila alamat pengirim request disamarkan dan tidak hanya mengirimkan ICM request pada sebuah network melainkan kebeberapa network. Tentu saja balasan yang diterima akan lebih besar lagi, tidak hanya sampai disitu. Pengirim menyamarkan identitasnya dengan cara memakai alamat IP orang lain.

**BAB III**

**PEMBAHASAN**

**3.1 Studi Kasus**

Seiring dengan perkembangan teknologi Internet, menyebabkan munculnya kejahatan yang disebut dengan “CyberCrime” atau kejahatan melalui jaringan Internet. Munculnya beberapa kasus “CyberCrime” di Indonesia, seperti penyebaran virus, hacking beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programmer komputer. Sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adanya CyberCrime yang semakin beragam & canggih telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet.

Adapun Cybercrime yang akan menjadi studi kasus kami kali ini, yaitu tentang *distributed denial of server attack* atau DDOS *attack*.

**3.2 Analisa Kasus**

Komputer merupakan salah satu perangkat yang sering digunakan untuk menyimpan file yang penting dan bersifat pribadi. Seiring dengan perkembangan teknologi yang semakin canggih maka keamanan komputer menjadi rawan untuk di bobol/dibajak oleh pihak-pihak yang tidak bertanggung jawab guna mengambil keuntungan pribadi. Penomena penyebaran virus dan hacking semakin marak terjadi. Berdasarkan tema studi kasus yang kami sampaikan sebelumnya, berikut pembahasan detailnya:

1. DDOS *Attack*

Modus yang digunakan pelaku kejahatan cybercrime ini yaitu, pelaku mencoba memancing korban untuk memberikan informasi akun BBM /E-mailnya kepada pelaku dengan iming-iming setelah korban memberikan informasi username dan password tersebut maka korban dapat mengakses konten yang disediakan oleh pelaku dengan mengklik tautan atau link yang telah disediakan oleh pelaku. Biasanya pelaku menawarkan konten yang bermuatan pornografi guna menarik minat korban. Namun tidak menutup kemungkinan modus pelaku yaitu dengan menawarkan konten-konten hiburan seperti, download lagu, games, dokumen, video dan sebagainya secara gratis.

Salah satu contoh kasus yang terjadi yaitu seperti di kutip dari situs bbc.com & dunia.tempo.co, adapun linknya seperti berikut:

<http://www.bbc.com/indonesia/dunia/2010/09/100923_iranviruskomputer.shtml>

<https://dunia.tempo.co/read/news/2013/03/01/116464583/virus-stuxnet-untuk-melumpuhkan-nuklir-iran>

1. Contoh Kasus

Adapun contoh kasus kejahatan internet yang baru-baru ini terjadi adalah penyerangan virus stuxnet buatan Amerika Serikat-Israel yang ditujukan kepada Iran. Para pakar mengatakan program virus Stuxnet yang

sangat rumit mengisyaratkan bahwa program komputer ini dibuat oleh "pemerintah satu negara".

Ini diyakini sebagai virus pertama yang dibuat dengan sasaran infrastruktur seperti pusat pembangkit listrik, pusat penjernihan air minum, dan unit-unit industri. Virus ini pertama kali diketahui Juni lalu dan sejak itu dipelajari dengan seksama.

"Fakta bahwa begitu banyak virus ini ditemukan di Iran dibanding wilayah lain di dunia membuat kami berpikir bahwa virus ini memang dengan sengaja ditujukan untuk Iran dan ada sesuatu hal yang sangat berharga bagi pembuat virus ini," ujar Liam O'Murchu dari perusahaan keamanan komputer Symantec, yang terus mengikuti perjalanan virus ini sejak ditemukan.

Sejumlah kalangan berspekulasi bahwa virus ini mungkin dibuat untuk mengacaukan pusat pembangkit listrik tenaga nuklir Bushehr milik Iran atau pusat pengayaan uranium di Natanz, Iran.

Akan tetapi, O'Murchu dan pihak lain seperti pakar keamanan Bruche Scheiner mengatakan saat ini belum cukup bukti untuk mengambil kesimpulan mengenai sasaran dan pembuat virus ini.

Stuxnet pertama kali diketahui oleh satu perusahaan keamanan di Belarus, namun kemungkinan besar sudah beredar sejak tahun 2009.

Virus ini menyerang sistem pengendali pabrik buatan Siemens. Tidak seperti virus komputer lain, virus ini menyerang sistem yang tidak terkoneksi dengan internet karena alasan keamanan.

Virus ini masuk ke mesin komputer dengan sistem operasi Windows lewat stik memori USB -yang biasa digunakan untuk memindahkan data komputer- yang sudah terkontaminasi virus itu.

Jika virus ini sudah masuk ke komputer yang tergabung dalam jaringan internal satu perusahaan, virus ini mencari konfigurasi khusus dari program komputer pengendali industri buatan Siemens.

Setelah berhasil membajaknya, kode ini bisa memprogram ulang program yang disebut PLC (programmable logic control) untuk memberi mesin yang dikendalikannya perintah-perintah baru.

"[PLC] menghidupkan dan mematikan mesin, suhu monitor, menghidupkan mesin pendingin jika satu katup mencapai suhu tertentu," ujar O'Murchu.

"Ini semua sebelumnya tidak pernah diserang."

Jika program virus ini tidak berhasil menemukan konfigurasi yang dimaksud, program ini secara relatif tidak berbahaya. Akan tetapi virus ini membuat banyak pihak bertanya-tanya karena kerumitan kode yang digunakan dan fakta bahwa virus ini menyatukan berbagai teknik berbeda.

"Terlalu banyak teknik baru dan tidak diketahui yang digunakan yang sebelumnya tidak pernah terjadi."

Dia menjelaskan salah satu teknik itu adalah upaya menyembunyikan diri di PLC dan penggunaan stik memori USB serta enam metode berbeda untuk menyebarkan diri. Sebagai tambahan virus ini memanfaatkan kerentangan Windows yang belum diketahui sebelumnya, yang dikenal dengan sebutan eksploitasi zero-day.

"Sangat jarang melihat satu serangan mempergunakan ekploitasi zero-day," ujar Mikko Hypponen, kepala peneliti perusahaan keamanan F-Secure.

"Stuxnet mempergunakan tidak hanya satu atau dua, tetapi empat."

Dia mengatakan penjahat dunia maya dan peretas (hacker) biasa sangat menghargai eksploitasi zero-day dan tidak akan "menyia-nyiakannya" dengan mempergunakan begitu banyak sekaligus. Microsoft telah mengatasi dua kerentanan itu.

Sangat jarang melihat satu serangan mempergunakan eksploitasi zero-day Mikko Hypponen O'Murchu sepakat dan mengatakan bahwa analisanya mengisyaratkan pembuat virus ini "berusaha keras".

"Ini adalah proyek yang sangat besar, sangat terencana dan memiliki biaya besar," ujarnya. "Virus ini memiliki terlalu banyak kode hanya untuk tersebar ke mesin-mesin itu."

Analisanya ini didukung oleh penyelidikan yang dilakukan oleh perusahaan keamanan internet lain dan pakar komputer.

"Dengan forensik yang kita miliki, terbukti bahwa Stuxnet adalah serangan sabotase terarah yang melibatkan pengetahuan di dalam," ujar Ralph Langer, pakar komputer industri dalam analisa yang diterbitkan di dunia maya.

"Ini bukan hacker yang tinggal di rumah orang tuanya. Bagi saya untuk melakukan serangan dalam tingkat ini diperlukan sumber daya besar yang menunjuk pada pemerintah negara," tulisnya.

Langer yang menolak diwawancara BBC menjadi pusat perhatian setelah menyebut bahwa sasaran Stuxnet adalah pusat nuklir Busherhr. Secara khusus dia menggarisbawahi satu foto yang dilaporkan diambil di dalam pusat nuklir itu yang menunjukkan bahwa virus ini digunakan untuk menyerang sistem kendali, meski hal itu "tidak dikonfigurasi dan mendapat izin secara benar". O'Muchu mengatakan tidak ada kesimpulan pasti dari ini semua. Akan tetapi dia berharap hal itu akan berubah ketika dia membeberkan analisanya dalam satu konperensi di Vancouver minggu depan.

"Kami tidak terbiasa dengan konfigurasi yang digunakan di industri yang berbeda," ujarnya.

Jadi dia berharap pakar lain bisa membeberkan penelitian mereka dan menunjuk konfigurasi yang dibutukan dan di mana konfigurasi itu digunakan.

Virus disebarkan melalui stik memori USB yang dipindah-pindah. Juru bicara Siemens, pembuat sistem yang menjadi sasaran, mengatakan tidak mau berkomentar atas "spekulasi mengenai sasaran virus ini".

Dia mengatakan pusat pembangkit listrik tenaga nuklir Iran dibangun dengan bantuan satu kontraktor Rusia dan Siemens tidak terlibat.

"Siemens tidak pernah terlibat dalam pembangunan Bushehr atau pusat nuklir di Iran, atau menjual program komputer atau pun program sistem pengendali," ujarnya. Siemens meninggalkan negara itu hampir 30 tahun lalu."

Siemens mengatakan hanya tahu soal 15 peristiwa di mana virus ini berhasil masuk ke sistem pengendali di pabrik-pabrik, sebagian besar di Jerman. Analisa secara geografis Symantec terhadap penyebaran virus itu juga mengkaji penyebarannya ke komputer pribadi.

"Tidak ada contoh kasus di mana operasi produksi terganggu atau pabrik tidak berfungsi," ujar juru bicara Siements. "Virus ini telah dibuang dalam kasus yang kami ketahui."

O'Murchu mengatakan ini bukan pertama kali satu virus komputer berdampak pada infrastuktur penting, meski sebagian besar kasus terjadi secara kebetulan karena virus yang tadinya dibuat untuk merusak sistem tertentu secara tidak sengaja menyebar ke sistem yang lebih besar.

Tahun 2009 pemerintah Amerika Serikat mengakui bahwa telah ditemukan program komputer yang bisa melumpuhkan jaringan listrik nasional. Dan Hypponen mengatakan dia tahu soal serangan -yang dilakukan lewat stik memori USB- terhadap sistem militer satu negara anggota NATO.

"Apakah serangan itu berhasil, kami tidak tahu," ujarnya.

1. Analisa kasus

Dari kasus sebelumnya, kita dapat menganalisa permasalahan yang terjadi dengan pendekatan 5W+1H. Pendekatan 5W+1H adalah pendekatan yang bisa membantu dalam analisa permasalahan. 5W+1H terdiri dari:

1. What (Apa)
2. Who (Siapa)
3. Where (Di mana)
4. When(Kapan)
5. Why(Kenapa)
6. How(Bagaimana)

Enam pertanyaan tersebut merupakan pertanyaan yang dapat membantu memecahkan masalah dan memicu ide-ide. Namun terkadang orang menggunakan atau mengartikan pertanyaan-pertanyaan tersebut secara salah, sehingga analisa yang dilakukan akan menjadi tidak maksimal. Dan berikut adalah analisa berdasarkan pendekatan 5w+1H:

1. What (Apa)

Kasus ini membahas tentang virus buatan Amerika-Israel yang bernama virus stuxnet yang ditujukan kepada Iran

1. Who (Siapa)

Pelaku dalam kasus ini adalah Amerika-Israel yang bekerja sama dalam pembuatan virus stuxnet, sedangkan korbannya yaitu Iran.

1. Where (Dimana)

Virus ini ditemukan pada komputer pemerintahan Iran.

1. When (Kapan)

Virus stuxnet dibuat pada tahun 2007, tahun 2009 pemerintah Amerika Serikat mengakui bahwa telah ditemukan program komputer yang bisa melumpuhkan jaringan listrik nasional, dan pada tahun 2013 virus ini menyerang Iran.

1. Why (Mengapa)

Karena Amerika Serikat berusaha menggagalkan program nuklir Iran sejak diaktifkan dibawah pemerintahan presiden Mahmoud Ahmadinejad

1. How (Bagaimana)

virus ini menyerang sistem yang tidak terkoneksi dengan internet karena alasan keamanan. Virus ini masuk ke mesin komputer dengan sistem operasi Windows lewat stik memori USB -yang biasa digunakan untuk memindahkan data komputer- yang sudah terkontaminasi virus itu.

**3.3 Analisa Cyber Law**

Berdasarkan studi kasus di atas maka pelaku dapat dijerat dengan undang-undang ITE nomor 19 tahun 2016 pasal 31 ayat 1,dan 2. Dengan bunyi pasal sebagai berikut:

Pasal 31 ayat (1)

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau

penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer

dan/atau Sistem Elektronik tertentu milik Orang lain.”

Pasal 31 ayat (2)

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas

transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.”

Pelanggaran terhadap UU ITE pasal 31 ayat1dan 2 sebagaimana tercantum pada pasal 45 UU ITE yang berbunyi:

Pasal 45 ayat (1)

“Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan

dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang

memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1)

dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak

Rp1.000.000.000,00 (satu miliar rupiah).”

Pasal 45 ayat (4)

“Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan

dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang

memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”

**BAB IV**

**PENUTUP**

**4.1 Kesimpulan**

Dari studi kasus penyerangan DDOS atau *Distributed Denal Of Server* yang telah kami bahas, antara cybercrime yang terjadi dan cyberlaw yang diterapkan pada kasus tersebut, untuk penerapannya menurut kami tergantung ketegasan dari pihak penegak hukum itu sendiri. Hukuman pidana maksimal 6 sampai tahun dan denda paling berat Rp. 1000.000.000,00 (satu miliar rupiah), apalagi jika keuntungan yang diperoleh pelaku tidak sebanding dengan hukuman yang didapatkan. Namun, hukuman tersebut bisa dikatakan lebih ringan apabila keuntungan yang didapatkan pelaku lebih besar.

Jadi ketika menerapkan suatu hukuman, tergantung dari seberapa besar dampak yang ditimbulkan dari kejahatan tersebut.

**DAFTAR PUSTAKA**

Amperiyanto, Tri.2008. P3K Virus Komputer. Jakarta: PT. Elex Media Komputindo.

<http://www.bbc.com/indonesia/dunia/2010/09/100923_iranviruskomputer.shtml>

<https://dunia.tempo.co/read/news/2013/03/01/116464583/virus-stuxnet-untuk-melumpuhkan-nuklir-iran>

<http://itdare.blogspot.co.id/2014/12/pengertian-cyber-crime-dan-jenis-jenis.html>

<https://id.wikipedia.org/wiki/Stuxnet>

<http://etikaprofesi.weebly.com/pengertian-cyber-law.html>

**LEMBAR PENILAIAN**

**Judul Makalah : Studi Kasus *Distributed Danial Of Server Attack***

**Mata Kuliah : Etika Profesi Teknologi Informasi Komunikasi**

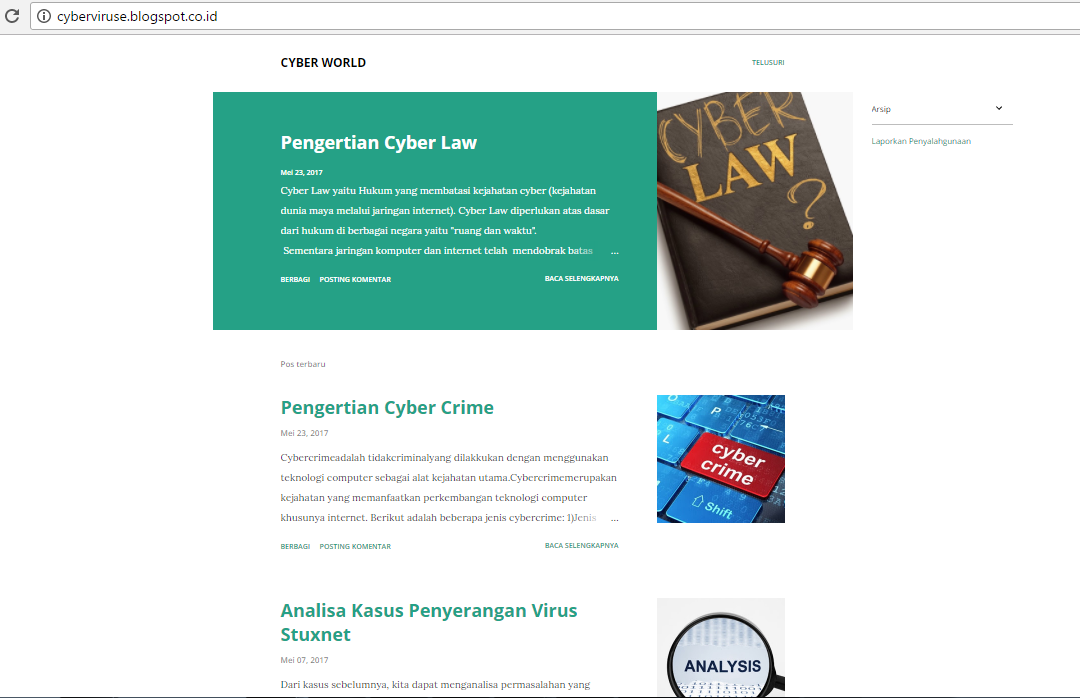
**Kelas : 12.6A.11**

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Nama | Nim | Nilai |
| 1. | Muhammad Husein | 1214 |  |
| 2. | Fikri Hidayat | 1214 |  |
| 3. | Rahmad Bani Adji | 1214 |  |
| 4. | Arif Trian Nugroho | 12146005 |  |
| 5. | Andro Julio | 1214 |  |

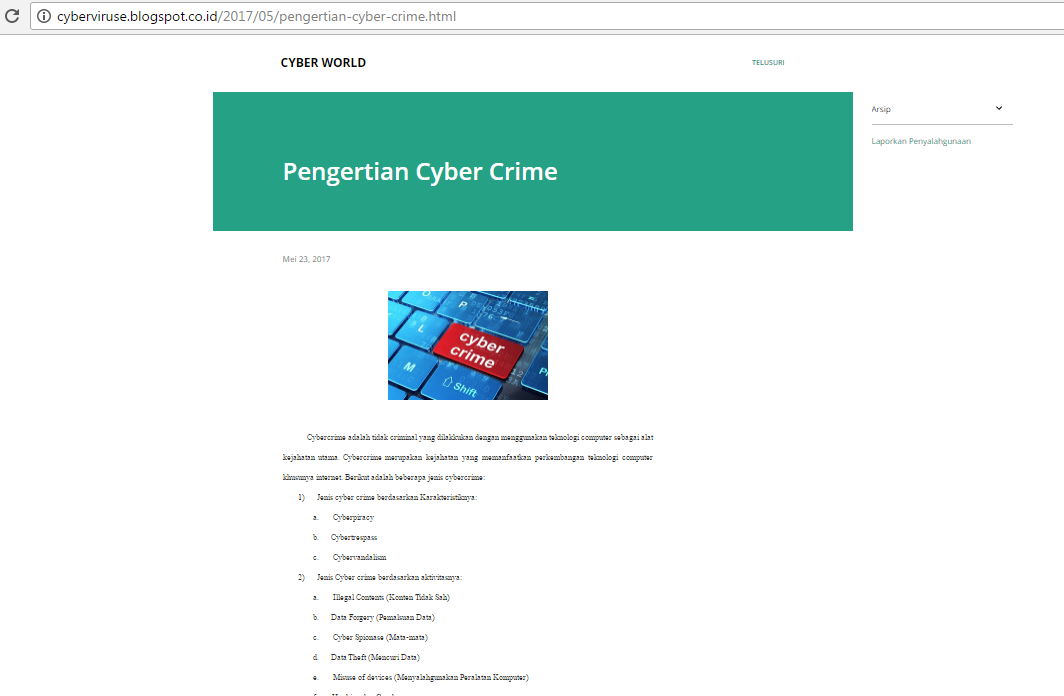
**CAPTURE BLOG**

Link: <http://cyberviruse.blogspot.co.id/>

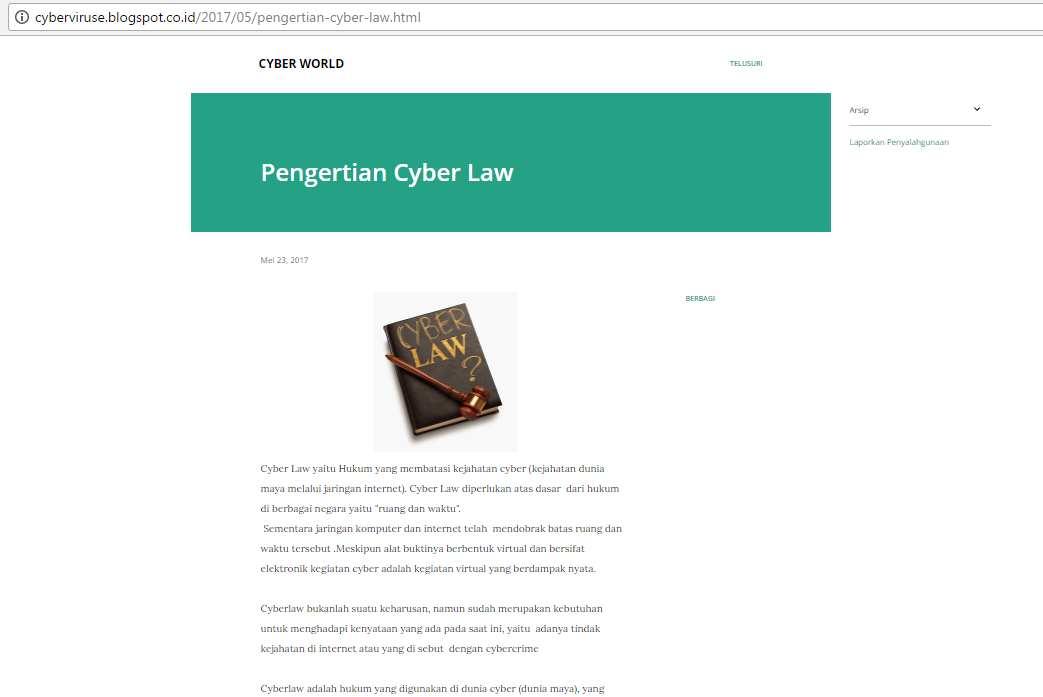
1. Tampilan Home



1. Artikel Pengertian CyberCrime



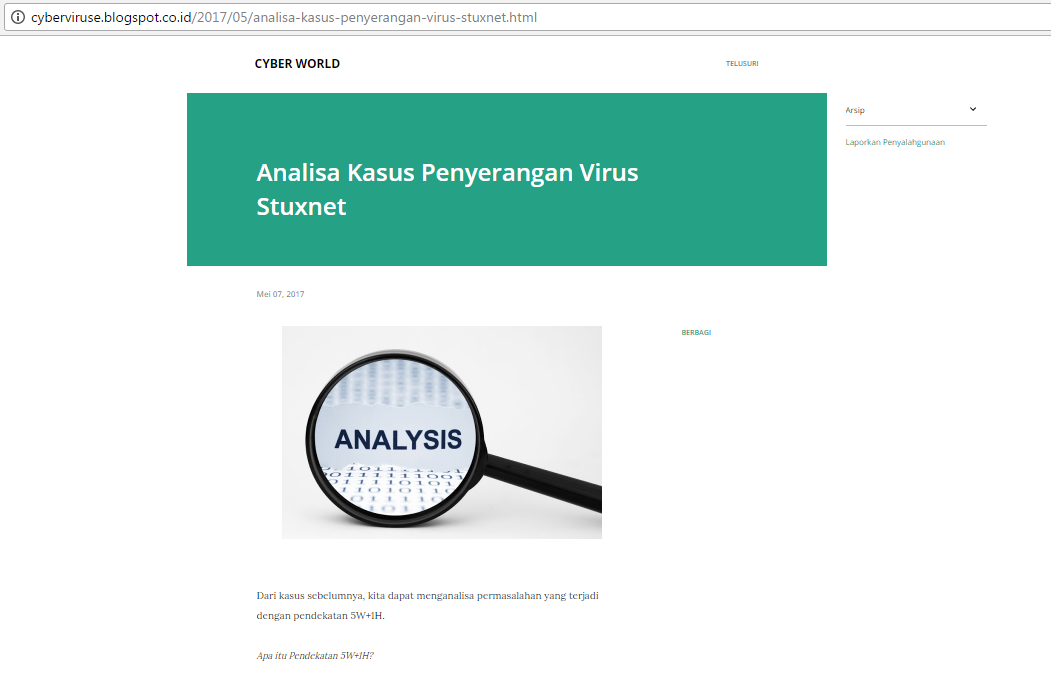
1. Artikel Pengertian Cyber Law



1. Artikel Pengertian Kasus Cyber Crime



1. Artikel Aanlis Kasus



**CURRICULUM VITAE**

***Data Pribadi***

Nama : Karel Junio

Tempat, Tanggal Lahir : Surabaya, 12 Juni 1996

Jenis Kelamin : Laki-Laki

Umur : 20 Tahun

Agama : Islam

Alamat : Jalan Teluk Angsan Permai No.137 Block D no.137

Kel.Bekasi Jaya Kec.Bekasi Timur Kota.Bekasi

Status : Belum Menikah

Telepon : 082113897135

Email : [kareljuniom@gmail.com](mailto:rafdiabi666@gmail.com)

*Latar Belakang*

* Formal

2002-2008 : SD Negeri Bekasi Jaya IX

2008-2011 : SMP Negeri 18 Bekasi

2011-2014 : SMK Karya Guna 1 Bekasi

 Jakarta, 23 Mei 2017

Penyusun

**Karel Junio**

Nim: 12140613

**CURRICULUM VITAE**

***Data Pribadi***

Nama : Abi Rafdi

Tempat, Tanggal Lahir : Bekasi, 26 Januari 1996

Jenis Kelamin : Laki-Laki

Umur : 21 Tahun

Agama : Islam

Alamat : Jalan Gunung Gede 9 No.60 Block C RT.05/13

Kel.Kayuringin Jaya Kec.Bekasi Selatan

Kota.Bekasi

Status : Belum Menikah

Telepon : 087888410616

Email : [rafdiabi666@gmail.com](mailto:rafdiabi666@gmail.com)

*Latar Belakang*

* Formal

2001-2007 : SD Negeri Kayuringin Jaya XVI

2007-2010 : SMP Negeri 7 Bekasi

2010-2013 : SMA Negeri 2 Bekasi

 Jakarta, 23 Mei 2017

Penyusun

**Abi Rafdi**

Nim: 12142600

**CURRICULUM VITAE**

***Data Pribadi***

Nama : Nadia Ayu Lestari

Tempat, Tanggal Lahir : Jakarta, 23 Juni 1996

Jenis Kelamin : Perempuan

Umur : 20 Tahun

Agama : Islam

Alamat : Jalan Delima V/9 No.149 Prumnas Klender

Kel.Malaka Sari Kec.Duren Sawit Kota.Jakarta

Status : Belum Menikah

Telepon : 082298067717

Email : [nadiaylst@gmail.com](mailto:rafdiabi666@gmail.com)

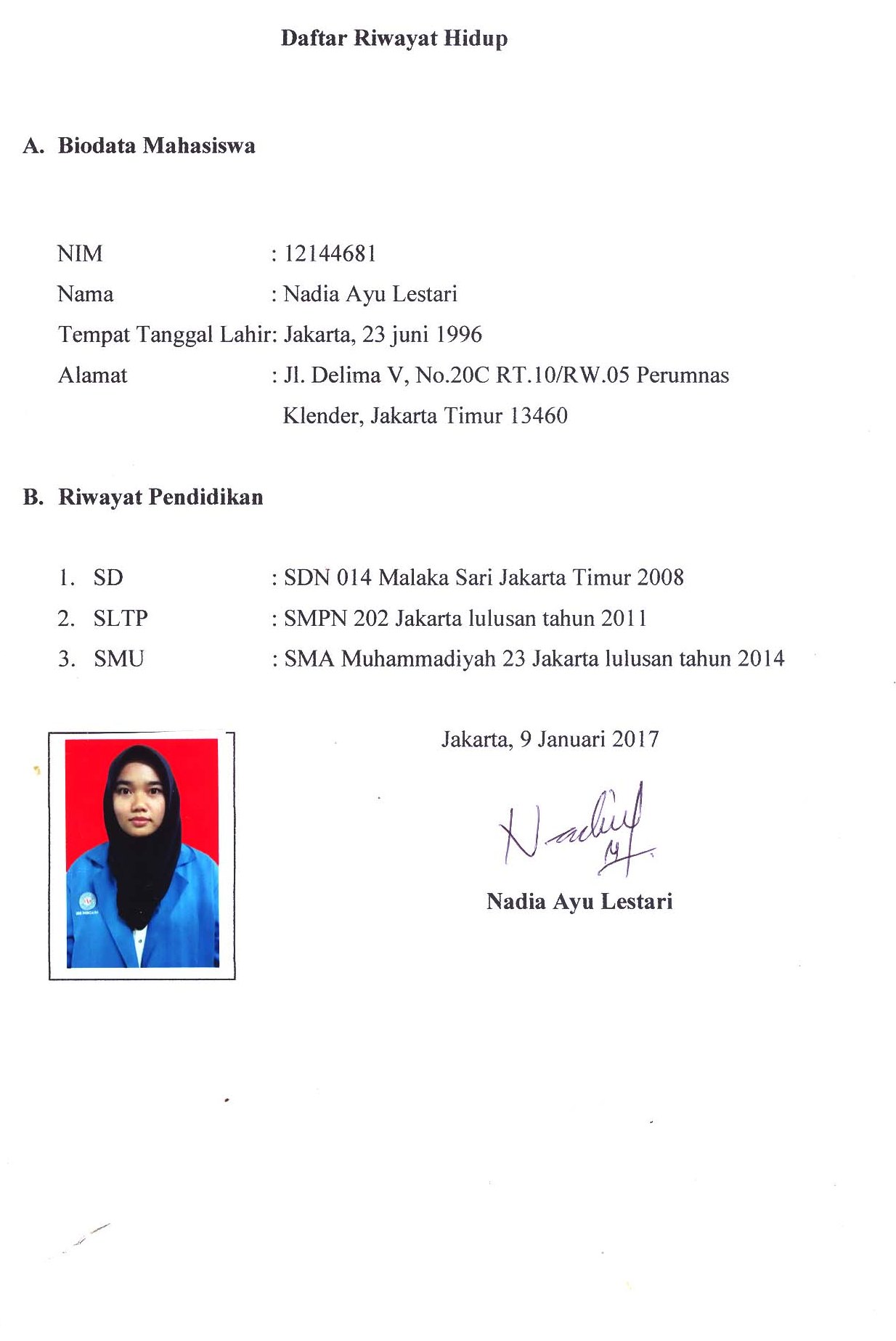
*Latar Belakang*

* Formal

2002-2008 : SD Negeri 014 Malaka Sari Jakarta Timur

2008-2011 : SMP Negeri 202 Jakarta

2011-2014 : SMA Muhammadiyah 23 Jakarta

 Jakarta, 23 Mei 2017

Penyusun

**Nadia Ayu Lestari**

Nim: 12144681

**CURRICULUM VITAE**

***Data Pribadi***

Nama : Abdillah

Tempat, Tanggal Lahir : Jakarta, 18 Maret 1997

Jenis Kelamin : Laki-Laki

Umur : 20 Tahun

Agama : Islam

Alamat : Kp. Rawa Bacang No.56 RT.007/014

Kel.Jati Rahayu Kec.Pondok Gede Kota.Bekasi

Status : Belum Menikah

Telepon : 081296683558

Email : [abdillah1827@gmail.com](mailto:rafdiabi666@gmail.com)

*Latar Belakang*

* Formal

2002-2008 : SD Negeri Cipinang Melayu 10 Pagi

2008-2011 : SMP Negeri 51 Jakarta

2011-2014 : SMA Negeri 50 Jakarta

 Jakarta, 23 Mei 2017

Penyusun

**Abdillah**

Nim: 12144774

**CURRICULUM VITAE**

*Data Pribadi*

Nama : Siska Siti Oktavia

Tempat, Tanggal Lahir : Jepara, 26-Oktober-1996

Jenis Kelamin : Perempuan

Umur : 20 Tahun

Agama : Islam

Alamat : Perumahan Grand Nusa Indah Blok T9 No3

Cileungsi, Bogor, Jawa Barat. 16820

Status : Belum Menikah

Telepon : 089633088247

Email : [siska.chikka@gmail.com](mailto:siska.chikka@gmail.com)

*Latar Belakang*

* Formal

2002-2008 : Madrasah Ibtidaiyah Bandengn

2008-2011 : SMP Negeri 1 Jepara

2011-2014 : SMA Negeri 1 Jepara

 Jakarta, 23 Mei 2017

Penyusun

**Siska Siti Oktavia**

Nim: 12146937