MAKALAH CYBER LAW & CYBER CRIME

LINK DOWNLOAD [273.45 KB]

MAKALAH
CYBER LAW & CYBER CRIME
Makalah ini dibuat
Sebagai bahan Presentasi Kelompok Mata kuliah Etika Profesi Teknologi Informasi Dan Komunikasi
(EPTIK)
Disusun Oleh:
12.4A.17
1. M Sarifal 12131664
2. Try Nurdiani 12132844
3. Seni Kurniasari 12133233
4. Dede Ruhimat 12133329
5. Annisa Rosyidah 12137388
AKADEMIK MANAJEMEN INFORMATIKA DAN KOMPUTER
BINA SARANA INFORMATIKA
TASIKMALAYA
2015

KATA PENGANTAR

Dengan memanjatkan puji dan syukur ke hadirat Allah S. W. T Yang Maha Esa, karena dengan Rahmat-Nya kami telah dapat menyelesaikan penyusunan Makalah Cyber Law & Cyber Crime Pada Etika Profesi Teknologi Informasi dan Komunikasi ini. Dan kami mengucapkan terima kasih pula untuk Dosen dan teman-teman sekalian yang telah mendukung dan membantu menyelesaikan makalah ini dengan sebaik mungkin. Makalah ini dibuat bertujuan untuk mendapatkan nilai UAS (Ujian Akhir Semester). Kami berharap semua pihak dapat mendukung makalah ini.

Kami menyadari bahwa makalah ini masih perlu ditingkatkan mutunya. Dan semoga makalah ini dapat bermanfaat untuk teman-teman yang membacanya. Oleh karena itu, saran dan kritik sangat kami harapkan. Tujuan pembuatan makalah ini adalah salah satu syarat untuk mendapat nilai UAS (Ujian Akhir Semester) terbaik pada studi ?Etika Profesi Teknologi Informasi dan Komunikasi? di AMIK BSI . Sebagai bahan penulisan, diambil dari proses observasi, dan wawancara serta beberapa narasumber yang mendukung pembuatan makalah ini.

Kami menyadari tanpa kerjasama yang baik dan dukungan semua pihak, maka makalah ini tidak akan berjalan dengan lancar. Oleh karena itu pada kesempatan ini kami ingin menyampaikan ucapan terima kasih kepada :

1. Allah SWT, yang telah memberi Rahmat-Nya kepada kami
untuk tetap bersabar dalam mengahadapi hidup ini.
2. Ibu Yanti , selaku Dosen pembimbing pada studi Etika Profesi
IT, yang banyak memberikan bimbingan pelajaran dan pengarahan kepada kami.
3. Kedua Orang Tua kami, yang telah memberikan dukungan
secara moril, materil dan do'anya.
4. Serta teman-teman yang telah turut serta dalam pembuatan tugas makalah ini hingga dapat terselesaikan . Kami menyadari bahwa pembuatan makalah ini masih banyak kekurangan , tapi kami berharap makalah ini dapat berguna untuk semuanya.

Akhirnya penulis berharap semoga makalah ini bermanfaat bagi semua pihak, meskipun dalam laporan ini masih banyak kekurangannya. Oleh sebab itu kritik dan saran yang membangun sangat penulis harapkan.

Penulis, 25 April 2015
Tasikmalaya

DAFTAR ISI

Halaman.

BAB I

PENDAHULUAN

1. 1 . Latar Belakang

Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Salah satu perkembangan teknologi yang sering digunakan dan dibutuhkan semua kalangan masyarakat adalah computer. Dengan computer seseorang dapat dengan mudah mempergunakannya, tetapi dengan adanya computer seseorang menggunakannya dengan ada hal yang baik dan tidaknya. Cyber crime dan cyber law dimana kejahatan ini sudah melanggar hukum dalam teknologi dan seseorang yang mengerjakannya dapat di kenakan hukum pidana dan perdata.

1. 2. Metode Penulisan

Makalah ini merupakan salah satu tugas untuk mendapatkan nilai pengganti UJian Akhir Semester (UAS) dalam mata kuliah Etika Profesi Teknologi Informasi & Komunikasi. Penyusunan malakah ini, menitikberatkan pada kegiatan melanggar hukum di dunia maya yang di sebut dengan ?Cyber Crime? dan ?Cyber Law?. Makalah ini merupakan hasil pengumpulan data dan informasi melalui media internet yang di dalamnya terdapat banyak artikel dan informasi yang menjelaskan tentang Cyber Crime & Cyber Law ini.

1. 3. Tujuan Penulisan

Makalah ini di susun agar pemahaman tentang tindak kejahatan melalui media internet dengan sebutan Cyber Crime dan Cyber Law ini menjadi lebih mudah di mengerti bagi setiap orang yang membacanya. Dan khususnya untuk para pengguna media online, makalah ini merupakan informasi yang harus diaplikasikan dalam menggunakan media internet sebagai wadah untuk melakukan berbagai aktifitas dengan baik dan hati-hati.

Makalah ini secara khusus ingin mengaplikasikan teori mata kuliah Etika Profesi Teknologi Informasi dan Komunikasi dengan

mencari referensi dan menyebarkan informasinya melalui desain blog, untuk lebih memahami tentang apa itu cybercrime dan Cyberlaw berikut karakteristiknya dan seluk beluknya, dan juga disediakan pula beberapa contoh kasus untuk bisa lebih menerangkan Cyberlaw. Selain itu, makalah ini juga dibuat untuk mendapatkan nilai Ujian Akhir Semester VI mata kuliah Etika Profesi Teknologi Informasi dan Komunikasi yang menggunakan Kurikulum Berbasis Kompetensi (KBK)

1.4 Sistematika penulisan

Sebelum membahas lebih lanjut, sebaiknya penulis menjelaskan dahulu secara garis besar mengenai sistematika penulisan, sehingga memudahkan pembaca memahami isi makalah ini. Dalam penjelasan sistematika penulisan makalah ini adalah :

Bab I Pendahuluan

Berisikan tentang :

1. 1 Latar belakang
1. 2 Metode Penulisan
1. 3 Tujuan Penulisan
1. 4 Sistematika Penulisan

Bab II Pembahasan

Berisikan tentang :

2. 1 Undang-undang ITE (Informasi dan Transaksi Eletronik)
2. 2 Pengertian Cyber crime
2. 3. Motif kegiatan Cyber Crime
2. 4. Faktor Penyebab
2. 5. Karakteristik Cyber Crime
2. 6. Jenis Cyber Crime
2. 7. Perkembangan Cyber Crime Di Indonesia
2. 8. Cara Penanganan Dan Contoh Kasus
2. 9 Pengertian Cyber law
2. 10. Ruang Lingkup Cyber Law
2. 11. Topik Seputar Cyber Law
2. 12. Asas-asas Cyber Law
2. 13. Contoh Kasus Cyber Law

Bab III Penutup

Berisikan tentang :

3. 1 Kesimpulan
3. 2 Saran

BAB II

LANDASAN TEORI

2.1. Cyber Crime

2.1.1. Pengertian Cyber Crime

Cyber crime adalah sebuah bentuk kriminal yang mana menggunakan internet dan komputer sebagai alat atau cara untuk melakukan tindakan kriminal. Masalah yang berkaitan dengan kejahatan jenis ini misalnya hacking, pelanggaran hak cipta, pornografi anak, eksploitasi anak, carding dan masih banyak kejahatan melalui media internet. Juga termasuk pelanggaran terhadap privasi ketika informasi rahasia hilang atau dicuri, dan lainnya.

Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit, confidence fraud, penipuan identitas, pornografi anak, dan lain-lain.

Sumber : http://dumadia.wordpress.com/2009/02/03/faktor-faktor-yang-mempengaruhi-terjadinya-cyber-crime/

2.1.2. Faktor Penyebab Cyber Crime

Faktor-faktor yang mempengaruhi cyber crime adalah :

1. Faktor Politik. Mencermati maraknya cyber crime yang terjadi di Indonesia dengan permasalahan yang dihadapi oleh aparat penegak, proses kriminalisasi di bidang cyber yang terjadi merugikan masyarakat. Penyebaran virus koputer dapat merusak jaringan komputer yang digunakan oleh pemerintah, perbankan, pelaku usaha maupun perorangan yang dapat berdampak terhadap kekacauan

dalam sistem jaringan. Dapat dipastikan apabila sistem jaringan komputer perbankan tidak berfungsi dalam satu hari saja akan mengakibatkan kekacauan dalam transaksi perbankan. Kondisi ini memerlukan kebijakan politik pemerintah Indonesia untuk menanggulangi cyber crime yang berkembang di Indonesia. Aparat penegak hukum telah berupaya keras untuk menindak setiap pelaku cyber crime, tapi penegakkan hukum tidak dapt berjalan maksimal sesuai harapan masyarakat karena perangkat hukum yang mengatur khusus tentang cyber crime belum ada. Untuk menghindari kerugian yang lebih besar akibat tindakan pelaku cyber crime maka diperlukan kebijakan politik pemerintah Indonesia untuk menyiapkan perangkat hukum khusus (lex specialist) bagi cyber crime. Dengan perangkat hukum ini aparat penegak hukum tidak ragu-ragu lagi dalam melakukan penegakan hukum terhadap cyber crime.

2. Faktor Ekonomi. Kemajuan ekonomi suatu bangsa salah satunya dipengaruhi oleh promosi barang-barang produksi. Jaringan komputer dan internet merupakan media yang sangat murah untuk promosi. Masyarakat dunia banyak yang menggunakan media ini untuk mencari barang-barang kepentingan perorangan maupun korporasi. Produk barang yang dihasilkan oleh indutri di Indonesia sangat banyak dan digemari oleh komunitas Internasional. Para pelaku bisnis harus mampu memanfaatkan sarana internet dimaksud. Krisis ekonomi yang melanda bangsa Indonesia harus dijadikan pelajaran bagi masyarakat Indonesia untuk bangkit dari krisis dimaksud. Seluruh komponen bangsa Indonesia harus berpartisipasi mendukung pemulihan ekonomi. Media internet dan jaringan komputer merupakan salah satu media yang dapat dimanfaatkan oleh seluruh masyarakat untuk mempromosikan Indonesia.

3. Faktor Sosial Budaya. Faktor sosial budaya dapat dilihat dari beberapa aspek, yaitu :

a. Kemajuan teknologi Informasi. Dengan teknologi informasi manusia dapat melakukan akses perkembangan lingkungan secara akurat, karena di situlah terdapat kebebasan yang seimbang, bahkan dapat mengaktualisasikan dirinya agar dapat dikenali oleh lingkungannya.

b. Sumber Daya Manusia. Sumber daya manusia dalam teknologi informasi mempunyai peranan penting sebagai pengendali sebuah alat. Teknologi dapat dimanfaatkan untuk kemakmuran namun dapat juga untuk perbuatan yang mengakibatkan petaka akibat dari penyimpangan dan penyalahgunaan. Di Indonesia Sumber Daya Pengelola teknologi Informasi cukup, namun Sumber Daya untuk memproduksi masih kurang. Hal ini akibat kurangnya tenaga peneliti dan kurangnya biaya penelitian dan apresiasi terhadap penelitian. Sehingga Sumber Daya Manusia di Indonesia hanya menjadi pengguna saja dan jumlahnya cukup banyak.

c. Komunitas Baru. Dengan adanya teknologi sebagai sarana untuk mencapai tujuan, di antaranya media internet sebagai wahana untuk berkomunikasi, secara sosiologis terbentuk sebuah komunitas baru di dunia maya.

Komunitas ini menjadim populasi gaya baru yang cukup diperhitungkan. Pengetahuan dapat diperoleh dengan cepat.

Sumber : http://dumadia.wordpress.com/2009/02/03/faktor-faktor-yang-mempengaruhi-terjadinya-cyber-crime/

2.1.3. Jenis-jenis Cyber Crime

1. Carding, Adalah kejahatan dengan menggunakan teknologi computer untuk melakukan transaksi dengan menggunakan card credit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil.dalam artian penipuan kartu kredit online.

2. Cracking, Kejahatan dengan menggunakan teknologi computer yang dilakukan untuk merusak system keamanan suatu system computer dan biasanya melakukan pencurian, tindakan anarkis begitu merekan mendapatkan akses. Biasanya kita sering salah menafsirkan antara seorang hacker dan cracker dimana hacker sendiri identik dengan perbuatan negative, padahal hacker adalah orang yang senang memprogram dan percaya bahwa informasi adalah sesuatu hal yang sangat berharga dan ada yang bersifat dapat dipublikasikan dan rahasia.Sedang Cracker identik dengan orang yang mampu merubah suatu karakteristik dan properti sebuah program sehingga dapat digunakan dan disebarkan sesuka hati padahal program itu merupakan program legal dan mempunyai hak cipta intelektual.

3. Joy computing, yaitu pemakaian komputer orang lain tanpa izin.

4. Hacking, yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal.

5. The trojan horse, yaitu manipulasi data atau program dengan jalan mengubah data atau intsruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau, dengan tujuan kepentingan pribadi atau orang lain.

6. Data leakage, yaitu menyangkut pembocoran data ke luar terutama mengenai data yang harus dirahasiakan.

7. Data diddling, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah input data atau output data.

8. To frustate data communication atau penyia-nyiaan data komputer.

9. Software piracy, yaitu pembajakan software terhadap hak cipta yang dilindungi Hak atas Kekayaan Intelektual (HaKI).

10. Cyber Espionage, Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang computerized.Biasaynya si

penyerang menyusupkan sebuah program mata-mata yang dapat kita sebut sebagai spyware.
11. Infringements of Privacy, Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.
12. Data Forgery, Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi ?salah ketik? yang pada akhirnya akan menguntungkan pelaku.
13. Unauthorized Access to Computer System and Service, Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.bagi yang belum pernah dengar, ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa website milik pemerintah RI dirusak oleh hacker.Kisah seorang mahasiswa fisipol yang ditangkap gara-gara mengacak-acak data milik KPU.dan masih banyak contoh lainnya.
14. Cyber Sabotage and Extortion, Merupakan kejahatan yang paling mengenaskan.Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai cyber-terrorism.
15. Offense against Intellectual Property, Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.Dapat kita contohkan saat ini.Situs mesin pencari bing milik microsoft yang konon di tuduh menyerupai sebuah situs milik perusahaan travel online.
16. Illegal Contents, Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah, dan sebagainya.Masih ingat dengan kasus prita mulyasari yang sampai saat ini belum selesai.Hanya gara-gara tulisan emailnya yang sedikit merusak nama baik sebuah institusi kesehatan swasta dia di seret ke meja hijau.
Sumber : http://it.ums.ac.id/?p=42
2.1.4. Dampak Cybercrime Terhadap Keamanan Negara
Berdasarkan studi kepustakaan yang kelompok kami lakukan mengenai Cyber Crime dan Cyber Law, beserta kasus-kasus yang pernah terjadi di Indonesia, kami melihat banyak dampak-dampak yang terjadi terhadap keamanan negara, dampak tersebut dapat disorot dalam aspek :
a. Kurangnya kepercayaan dunia terhadap Indonesia. Semakin banyaknya cybercrime yang ada di Indonesia, mencerminkan gagalnya pemerintah Indonesia untuk mengamankan negeri ini dari kriminalisme, khususnya di dunia maya (cyberspace). Akibatnya, kepercayaan dunia terhadapa keamanan di Indonesia menjadi berkurang.
b. Berpotensi menghancurkan negara. Jika tidak ada tindakan yang tegas dalam mengantisipasi cybercrime, sama saja seperti ?Bunuh Diri?.
c. Keresahan masyarakat pengguna jaringan komputer.
BAB III
PEMBAHASAN
3.1. Tips dan Cara Mengantisipasi Cybercrime
3.1.1. Pengamanan Internet
1. Melindungi Komputer
Sudah pasti hal ini mutlak Anda lakukan. Demi menjaga keamanan, paling tidak Anda harus mengaplikasikan tiga program, yaitu

antivirus, antispyware, dan firewall. Fungsinya sudah jelas dari ketiga aplikasi tersebut. Antivirus sudah pasti menjaga perangkat komputer Anda dari virus yang kian hari beragam jenisnya.

2. Melindungi Identitas

Jangan sesekali memberitahukan identitas seperti nomor rekening, nomor kartu penduduk, tanggal lahir dan lainnya. Karena hal tersebut akan sangat mudah disalah gunakan oleh pelaku kejahatan internet hacker.

3. Selalu Up to Date

Cara dari para pelaku kejahatan saat melakukan aksinya yaitu dengan melihat adanya celah-celah pada sistem komputer Anda. Karena itu, lakukanlah update pada komputer. Saat ini beberapa aplikasi sudah banyak menyediakan fitur update berkata secara otomatis. Mulai dari aplikasi antivirus dan aplikasi-aplikasi penunjang lainnya.

4. Amankan E-mail

Salah satu jalan yang paling mudah dan sering digunakan untuk menyerang adalah e-mail. Waspadalah setiap kali Anda menerima e-mail. Pastikan Anda mengetahui identitas dari si pengirim e-mail. Jika Anda sudah menerima e-mail dengan pesan yang aneh-aneh, sebaiknya jangan Anda tanggapi. Waspadai e-mail palsu yang sekarang banyak digunakan untuk menipu korban.

5. Melindungi Account

Gunakan kombinasi angka, huruf, dan simbol setiap kali Anda membuat kata sandi. Ini bertujuan agar kata sandi Anda tidak mudah diketahui atau dibajak. Namun jangan sampai Anda sendiri lupa kata sandi tersebut. Menggunakan password yang sulit merupakan tindakan cerdas guna menghindari pencurian data.

6. Membuat Salinan

Sebaiknya para pengguna komputer memiliki salinan dari dokumen pribadinya, entah itu berupa foto, musik, atau yang lainnya. Ini bertujuan agar data Anda masih tetap bisa terselamatkan bila sewaktu-waktu terjadi pencurian data atau ada kesalahan pada sistim komputer Anda.

7. Cari Informasi

Meskipun sedikit membosankan, tapi ini penting buat Anda. Dengan memantau perkembangan informasi pada salah satu penyedia jasa layanan keamanan internet juga diperlukan, salah satunya adalah pada National Cyber Alert System yang berasal dari Amerika, Anda diharapkan dapat mengetahui jenis penyerangan yang sedang marak terjadi. Dan dari situ pula Anda akan mendapatkan informasi bagaimana menanggulangi penyerangan tersebut bila terjadi pada Anda.

3.1.2. Penanganan Cyber Crime

Untuk menjaga keamanan data-data pada saat data tersebut dikirim dan pada saat data tersebut telah disimpan di jaringan komputer, maka dikembangkan beberapa teknik pengamanan data. Beberapa teknik pengamanan data yang ada saat ini antara lain:

1. Internet Firewall adalah Jaringan komputer yang terhubung ke Internet perlu dilengkapi dengan internet Firewall. Internet Firewall berfungsi untuk mencegah akses dari pihak luar ke sistem internal. Dengan demikian data-data yang berada dalam jaringan komputer tidak dapat diakses oleh pihak-pihak luar yang tidak bertanggung jawab. Firewall bekerja dengan 2 cara: menggunakan filter dan proxy. Firewall filter menyaring komunikasi agar terjadi seperlunya saja, hanya aplikasi tertentu saja yang bisa lewat dan hanya komputer dengan identitas tertentu saja yang bisa berhubungan. Firewall proxy berarti mengizinkan pemakai dari dalam untukmengakses internet seluas-luasnya, namun dari luar hanya dapat mengakses satu computer tertentu saja.

2. Kriptografi adalah seni menyandikan data. Data yang akan dikirim disandikanterlebih dahulu sebelum dikirim melalui internet. Di komputer tujuan, data tersebut dikembalikan ke bentuk aslinya sehingga dapat dibaca dan dimengerti oleh penerima. Data yang disandikan dimaksudkan agar apabila ada pihak-pihak yang menyadap pengiriman data, pihak tersebut tidak dapat mengerti isi data yang dikirim karena masih berupa kata sandi. Dengan demikian keamanan data dapat dijaga. Ada dua proses yang terjadi dalam kriptografi, yaitu proses enkripsi dan dekripsi. Proses enkripsi adalah proses mengubah data asli menjadi data sandi, sedangkan proses dekripsi adalah proses megembalikan data sandi menjadi data aslinya. Data aslin atau data yang akan disandikan disebut dengan plain text, sedangkan data hasil penyadian disebut cipher text. Proses enkripsi terjadi di komputer pengirim sebelum data tersebut dikirimkan, sedangkan proses dekripsi terjadi di komputer penerima sesaat setelah data diterima sehingga si penerima dapat mengerti data yang dikirim.

3. Secure Socket Layer (SSL) Jalur pengiriman data melalui internet melalui banyak transisi dan dikuasai oleh banyak orang. Hal ini menyebabkan pengiriman data melalui Internet rawan oleh penyadapan. Maka dari itu, browser di lengkapi dengan Secure Socket Layer yang berfungsi untuk menyandikan data. Dengan cara ini, komputer-komputer yang berada di antara komputer pengirim dan penerima tidak dapat lagi membaca isi data.

3.1.3. Penegakan Hukum

1. Undang-Undang Nomor 11 Tahun 2008 Tentang Internet & Transaksi Elektronik (ITE)Undang-undang ini, yang telah disahkan

dan diundangkan pada tanggal 21 April 2008, walaupun sampai dengan hari ini belum ada sebuah PP yang mengatur mengenai teknis pelaksanaannya, namun diharapkan dapat menjadi sebuah undang-undang cyber atau cyberlaw guna menjerat pelaku-pelaku cybercrime yang tidak bertanggungjawab dan menjadi sebuah payung hukum bagi masyarakat pengguna teknologi informasi guna mencapai sebuah kepastian hukum.

a. Pasal 27 UU ITE tahun 2008 : Setiap orang 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. Ancaman pidana pasal 45(1) KUHP. Pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah). Diatur pula dalam KUHP pasal 282 mengenaikejahatan terhadap kesusilaan.

b. Pasal 28 UU ITE tahun 2008 : Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.

c. Pasal 29 UU ITE tahun 2008 : Setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasaan atau menakut-nakuti yang dutujukkan secara pribadi (Cyber Stalking). Ancaman pidana pasal 45 (3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 29 dipidana denganpidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).

d. Pasal 30 UU ITE tahun 2008 ayat 3 : Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau system elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol system pengaman (cracking, hacking, illegal access). Ancaman pidana pasal 46 ayat 3 setiap orang yang memebuhi unsure sebagaimana dimaksud dalam pasal 30 ayat 3 dipidana dengan pidana penjara paling lama 8 (delapan) dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

e. Pasal 33 UU ITE tahun 2008 : Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya system elektronik dan/atau mengakibatkan system elektronik menjadi tidak bekerja sebagaiman mestinya.

f. Pasal 34 UU ITE tahun 2008 : Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki.

g. Pasal 35 UU ITE tahun 2008 : Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut seolah-olah data yang otentik (Phising = penipuan situs).

2. Kitab Undang Undang Hukum Pidana

a. Pasal 362 KUHP yang dikenakan untuk kasus carding.

b. Pasal 378 KUHP dapat dikenakan untuk penipuan.

c. Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkannya.

d. Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama
baik dengan menggunakan media Internet.

e. Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi.yang dilakukan secaraonline di Internet dengan penyelenggara dari Indonesia

f. Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi.

g. Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang.

h. Pasal 406 KUHP dapat dikenakan pada kasus deface atau hacking yang membuat sistem milik orang lain.

3. Undang-Undang No 19 Tahun 2002 tentang Hak Cipta.

Menurut Pasal 1 angka (8) Undang ? Undang No 19 Tahun 2002 tentang Hak Cipta, program komputer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut.

4. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi Menurut Pasal 1 angka (1) Undang ? Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya.

5. Undang-Undang No 8 Tahun 1997 tentang Dokumen Perusahaan Undang-Undang No. 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan. Misalnya Compact Disk ? Read Only Memory (CD ? ROM), danWrite ? Once -Read ? Many (WORM), yang

diatur dalam Pasal 12 Undang-Undang tersebutsebagai alat bukti yang sah.
6. Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang Jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan.
7. Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana TerorismeUndang-Undang ini mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu. Digital evidence atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme. karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di Internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui pelacakan terhadap Internet lebih sulit dibandingkan pelacakan melalui handphone. Fasilitas yang sering digunakan adalah e-mail dan chat roomselain mencari informasi dengan menggunakan search engine serta melakukan propaganda melalui bulletin board atau mailing list.
3.2. Study Kasus
Di indonesia pelanggaran kasus diinternet semakin meningkat setiap tahunya berikut total kerugian masyarakat dari kasus cyber crime ini tahun 2011 mencapai Rp4,8 miliar, tahun 2012 mencapai Rp5, 2 miliar dan USD 56.448. "Sedangkan tahun 2013 mencapai Rp848 juta lebih," kata Kapolda Metro sembari mengingatkan masyarakat berhati-hati dalam melakukan transaksi secara online. nah dibawah ini kami akan membahas sedikit contoh kasus yang terjadi di Indonesia silahkan disimak.
3.2.1. Kasus Penipuan Bisnis Online
ini terjadi pada tahun 2013, tepatnya Kamis (14/03/2013). Seorang mahasiswa salah satu universitas negeri yang ada di Bandung dijerat dengan undang-undang karena melakukan penipuan dalam menjalankan bisnis online-nya. Menurut sebuah artikel di Tempo.co, Kepolisian Daerah Jawa Barat menangkap KM (21) atas sebuah kejahatan penipuan online dengan modus investasi valuta asing atau foreign exchange.
KM menawarkan keuntungan besar lewat situsnya pandawainvesta.com. Tak tanggung-tanggung, KM membuka kantor cabang di daerah Cicaheum, Bandung, agar ?calon korban'-nya lebih percaya dengan apa yang ia tawarkan. Ia menjalankan bisnis ini sejak November 2012 dan telah memperdaya 338 nasabah dengan total kerugian yang dihasilkan sekitar 40 miliar rupiah.
Paket keuntungan yang KM tawarkan bervariasi. Mulai dari 50 persen, 70 persen, 100 persen, hingga 300 persen. Semakin banyak uang yang diinvestasikan oleh nasabahnya, semakin besar keuntungan yang dijanjikan oleh KM.
Pengusutan kasus KM didasari oleh laporan seorang nasabahnya. Kepala Bidang Hubungan Masyarakat Komisaris Besar Martinus Sitompul mengatakan, nasabah-nasabah bisnis KM berasal dari berbagai daerah. Ada yang berasal dari Bandung, Jakarta, Bogor, Batam, Surabaya, hingga Samarinda. Kombes Martinus juga menyatakan, KM dijerat dengan Undang-Undang tentang Informasi dan Transaksi Elektronik dengan ancaman hukuman enam tahun dan KUHP tentang Penipuan dengan ancaman hukuman empat tahun.
Analisa Kasus
Penipuan bisnis online terjadi melalui situs pandawainvesta.com. Kasus penipuan ini termasuk sebagai tindakan murni kejahatan didunia maya, karena penyelenggara dengan sengaja membuat situs untuk menipu dan menarik perhatian pembaca situs tersebut. Penipuan bisnis online termasuk kedalam cybercrime illegal content karena pelaku memasukan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum. Sasaran dari penipuan bisnis online ini adalah individu dimana pelaku menyebarkan informasi tersebut dengan maksud untuk memperoleh keuntungan secara material.
Biasanya faktor yang mempengaruhi kejahatan ini adalah faktor ekonomi dan sosial budaya karena tingkat pengangguran dan kesejahteraan sosial masih kurang dimana motif pelaku adalah mengeruk keuntungan material yang dilakukan menggunakan fasilitas internet.
Badan Hukum
Berdasarkan tindak kejahatan yang pelaku lakukan, maka pelaku dapat terjerat hukum. Beberapa pasal yang menjeratnya, antara lain:
1.Pasal 28 UU No. 11/2008 tentang ITE.
Pada pasal ini terdapat aturan secara khusus tentang tindak pidana tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
2.Pasal 378 KUHP tentang penipuan, dengan hukuman pidana penjara 4 (empat) tahun.
3.2.2. Kasus Tentang Penggelapan Uang di Bank melalui Komputer

Pada tahun 1982 telah terjadi penggelapan uang di bank melalui komputer sebagaimana diberitakan ?Suara Pembaharuan? edisi 10 Januari 1991 tentang dua orang mahasiswa yang membobol uang dari sebuah bank swasta di Jakarta sebanyak Rp. 372. 100. 000, 00 dengan menggunakan sarana komputer. Perkembangan lebih lanjut dari teknologi komputer adalah berupa computer network yang kemudian melahirkan suatu ruang komunikasi dan informasi global yang dikenal dengan internet. Pada kasus tersebut,
Analisa Ksaus
kasus ini modusnya adalah murni criminal, kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan.
Badan Hukum
Penyelesaiannya, karena kejahatan ini termasuk penggelapan uang pada bank dengan menggunakan komputer sebagai alat melakukan kejahatan. Sesuai dengan undang-undang yang ada di Indonesia maka, orang tersebut diancam dengan pasal 362 KUHP atau Pasal 378 KUHP, tergantung dari modus perbuatan yang dilakukannya
Bunyi Pasal 362 KUHP
barang siapa dengan sengaja mengambil barang yang sepenuhnya atau sebagian milik orang lain dengan melawan hukum maka dihukum sebagai pencurian dengan ancaman pidana penjara paling lama 5 th atau denda paling banyak Rp. 900, 00
.
3.2.3.Kasus Situs Resmi Kepolisian Di-hack
Kepolisian menyelidiki pelaku peretasan (hacking) situs resmi kepolisian yang beralamat di http://www.polri.go.id. ?Kami akan selidiki dan cari pelakunya,? kata Kepala Divisi Hubungan Masyarakat Markas Besar Kepolisian Republik Indonesia, Inspektur Jenderal Polisi Anton Bahrul Alam, Senin, 16 Mei 2011.
Halaman situs resmi kepolisian, hingga pukul 17.00 WIB sulit diakses. Pengunjung diarahkan ke alamat http:// http://www.polri.go.id/backend/index.html yang berisi gambar dua orang mengangkat bendera di atas bukit. Kemudian muncul tulisan berwarna hitam dengan seruan jihad.
Analisa kasus
Kasus ini hacker memblok situ resmi sehingga situs tersebut sulit diakses untuk bebetapa saat .
Badan Hukum
Hukum dari kasus ini yakni Pasal 22 dan 60 UU no. 36 tahun 1999 tentang Telekomunikasi untuk tindakan Domain Hijacking. Dan Pasal 406 KUHP dikenakan pada kasus deface atau hacking yang membuat sistem milik orang lain, seperti website atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya
3.2.4.Kasus Perjudian di internet(gambling)
Polda metro jaya menangkap seorang pelaku judi online didepan rumah sakitnHusada dijalan Mangga besar raya ,jakarta barat. Polsi melacak asal situs yang ternyata berasal dari luar negri tersebut.
Direktur reserse kriminal umum polda merto jaya, kombes tony herwanto ,menjelaskan pelaku menggunaka situs www.aseanbet.com sebagai media judi. Melalui situs tsb pelaku menjaring oranguntk berjudi di dunia maya dengan cara menebak skor permainan bola.
Hasil judi tsb keluar setiap selasa dan kamis, jika menang uang hasil judi akan masuk ke rekening pemain dan jka kalah akan masuk ke rekening bos pelaku. Polisi masih mengejar keberadaan pemilik situs judi dengan melacak internet protocol (IP) yang ternyata berasal dari luar negri.
?IP adress menunjukan berasal dari luar negri bukan indonesia kemungkinan berasal dari filipina atau singapura,? kata tony herwanto dikantornya minggu 16 desember 2012
Polisi berhasil menyita sejumlah barang bukti seperti dua unit laptop satu unit handphone satu unit unit modem satu unit buku tabungan bca a/n hendarto sunjoyo dan kartu atm atas nama budi tamsir satu buah buku catatan dan dua buah key(token) bca.
Analisa kasus:
Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi (TIK) telah pula menyebabkan hubungan dunia menjadi tanpa batas dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat.
Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum. Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan (TIK). Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika.
Istilah lain yang juga digunakan adalah hukum teknologi informasi, hukum dunia maya, dan hukum mayantara. Istilah tersebut lahir

mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Badan Hukum

Kasus judi online seperti yang dipaparkan diatas setidaknya bisa dijerat dengan 3 pasal dalam UU Informasi dan Transaksi Elektonik (ITE) atau UU No. 11 Tahun 2008. Selain dengan Pasal 303 KUHP menurut pihak Kepolisian diatas, maka pelaku juga bisa dikenai pelanggaran Pasal 27 ayat 2 UU ITE, yaitu ?Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian?.

Oleh karena pelanggaran pada Pasal tersebut maka menurut Pasal 43 ayat 1, yang bersangkutan bisa ditangkap oleh Polisi atau ?Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang?Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik?. Sementara sanksi yang dikenakan adalah Pasal 45 ayat 1, yaitu ?Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).?

3.2.5.Kasus Pencemaran nama baik café xxx

Baru-baru ini ada kasus pencemaran nama baik sebuah cafe di Surabaya sebut saja (X) tidak puas akan fasilitas dan pelayanan di café tersebut. kemudian X menulis atau membuat status disalah satu jejaring sosial. akibat tulisannya yang menjelekan cafe sehingga pemilik café merasa keberatan maka pemilik café melaporkannya pada pihak berwajib.

Analisa Kasus

Kasus ini terjadi karena ketidakpuasan pelanggan terhadap pelayanan di sebuah café yang dungkapkan lewat media sosial.

Badan Hukum

Akibat tulisannya itu X dikenakan UU ITE yaitu mengenai pencemaran nama baik pasal 27 ayat(3) UU ITE ?setiap orang dengan sengaja dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang bermuatan penghinaan dan/atau pencemaran nama baik?.

Untungnya pemilik café mau diajak berdamai dengan syarat X terkena denda dan X harus menulis pernyataan di jejaring sosial yang isinya meminta maaf dan harus memulihkan nama baik café tersebut selama 10 hari.

3.2.6.Kasus penyebaran video porno

Kasus ini terjadi saat ini dan sedang dibicarakan banyak orang, kasus video porno Ariel ?PeterPan? dengan Luna Maya dan Cut Tari, video tersebut di unggah di internet oleh seorang yang berinisial ?RJ' dan sekarang kasus ini sedang dalam proses.

Analisa kasus

Menurut kami seharunya Ariel, Luna dan Cut Tari tidak melakukan hala-hal yang tidak melanggar norma dan etika di agama,bangsa dan Negara. Kesalahan mereka pun bertambah karena apa yang mereka lakukan di dokumentasikan. Untuk seharusnya tidak mencampuri urusan pribadi dengan melakukan penyebaran video lewat internet, karena bukan hanya orang-orang dewasa yang dapat melihat tapi anak kecil pun bisa melihatnya.Pada kasus tersebut, modus sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut.

Badan Hukum

Penyelesaian kasus ini pun dengan jalur hukum, penunggah dan orang yang terkait dalam video tersebut pun turut diseret pasal-pasal sebagai berikut, Pasal 29 UURI No. 44 th 2008 tentang Pornografi Pasal 56, dengan hukuman minimal 6 bulan sampai 12 tahun. Atau dengan denda minimal Rp 250 juta hingga Rp 6 milyar. Dan atau Pasal 282 ayat 1 KUHP.

BAB III

PENUTUP

3. 1. Kesimpulan

Di dunia ini banyak hal yang memiliki dualisme yang kedua sisinya saling berlawanan. Seperti teknologi informasi dan komunikasi, hal ini diyakini sebagai hasil karya cipta peradaban manusia tertinggi pada zaman ini. Namun karena keberadaannya yang bagai memiliki dua mata pisau yang saling berlawanan, satu mata pisau dapat menjadi manfaat bagi banyak orang, sedangkan mata pisau lainnya dapat menjadi sumber kerugian bagi yang lain, banyak pihak yang memilih untuk tidak berinteraksi dengan teknologi informasi dan komunikasi. Sebagai manusia yang beradab, dalam menyikapi dan menggunakan teknologi ini, mestinya kita dapat

memilah mana yang baik, benar dan bermanfaat bagi sesama, kemudian mengambilnya sebagai penyambung mata rantai kebaikan terhadap sesama, kita juga mesti pandai melihat mana yang buruk dan merugikan bagi orang lain untuk selanjutnya kita menghindari atau memberantasnya jika hal itu ada di hadapan kita.

3. 2. Saran

Cybercrime adalah bentuk kejahatan yang mestinya kita hindari atau kita berantas keberadaannya. Cyberlaw adalah salah satu perangkat yang dipakai oleh suatu negara untuk melawan dan mengendalikan kejahatan dunia maya (cybercrime) khususnya dalam hal kasus cybercrime yang sedang tumbuh di wilayah negara tersebut. Seperti layaknya pelanggar hukum dan penegak hukum. Demikian makalah ini kami susun dengan usaha yang maksimal dari tim kami, kami mengharapkan yang terbaik bagi kami dalam penyusunan makalah ini maupun bagi para pembaca semoga dapat mengambil manfaat dengan bertambahnya wawasan dan pengetahuan baru setelah membaca tulisan yang ada pada makalah ini. Namun demikian, sebagai manusia biasa kami menyadari keterbatasan kami dalam segala hal termasuk dalam penyusunan makalah ini, maka dari itu kami mengharapkan kritik atau saran yang membangun demi terciptanya penyusunan makalah yang lebih sempurna di masa yang akan datang. Atas segala perhatiannya kami haturkan terimakasih

DAFTAR PUSTAKA

http://teknoinfo.web.id/undang-undang-baru-di-indonesia/ http://id.wikipedia.org/wiki/Kejahatan_dunia_maya/
http://en.wikipedia.org/wiki/Cyber_crime/ http://id.wikipedia.org/wiki/Perangkat_perusak/
http://abangs03.wordpress.com/2011/10/22/hello-world/
http://ihsanirawan001.blogspot.com/2013/10/contoh-study-kasus-cyber-crime-dan.html
http://komputerteknik07.blogspot.com/2013/10/makalah-pembahasan-cyber-crime-dan2655. html
http://komputerteknik07. blogspot. com/2013/10/contoh-kasus-cyber-law. html
http://timcyber. blogspot. com/2012/11/8-contoh-kasus-cyber-crime-dan. html
http://etikabsi124j11.blogspot.com/p/blog-page_1.html
http://tekno.kompas.com/read/2014/03/14/0915456/kesal.pendiri.facebook.telepon.presiden.obama
http://tekno.kompas.com/read/2013/11/18/1640492/5.model.ponsel.pejabat.indonesia.yang.disadap.australia
http://tekno.kompas.com/read/2012/05/06/16372714/fbi.ingin.sadap.facebook.gmail.ym.dan.skype