Nama : Ihfan Adnan Maulana

NIM : 18.12.0120

1. Contoh Pelanggaran Ceyber Law di Indonesia (selain di contohkan)?

**Contoh Kasus :**

1. **Ilegal Access**

Illegal akses merupakan salah satu tindak krimal dalam IT yang dikenal sebagai cyber crime, para heacker mengakses situs milik orang lain yang bertujuan untuk mengambil keuntungan sendiri tanpa memikirkan nasib korban, salah satunya adalah situs Mantan Presiden Republik Indonesia Susilo Bambang Yudhyono  yang belum lama ini kena retas.

**Pembobol situs SBY segera disidang**

Rabu,  6 Maret 2013  −  20:32 WIB

Presiden Susilo Bambang Yudhoyono (Ist)

**Sindonews.com** – Wildan Yani Ashari (20), seorang remaja asal Dusun Krajan Desa Balung Lor, Kecamataan Balung, ditangkap Tim Cyber Crime Mabes Polri beberapa waktu lalu, segera disidangkan. “Iya, ada komandan di Mabes Polri yang menyampaikan kepada saya kalau berkas penyidikan sudah tahap kedua dan sudah dikirim ke Kejaksaan Negeri Jember,” kata ayah Wildan, Ali Jakfar K, ketika dihubungi SINDO, di Yogyakarta, Rabu (6/3/2013). Menurut dia, jika berkas penyidikan sudah diserahkan dan dikirim ke Kejari Jember, maka tidak lama lagi proses sidang dugaan kejahatan dunia maya akan segera dimulai. Ali mengatakan, Wildan saat ini masih berada di Mabes Polri untuk menjalani tahanan dan pemberkasan.

“Namun Wildan di sana diperlakukan dengan baik kok. Bahkan di Mabes sekarang membantu perbaikan *server* milik Mabes dan masih bisa online dengan laptopnya,” ucapnya.

Sebelumnya, Wildan diduga sebagai pelaku pembobol situs resmi Presiden Susilo Bambang Yudhoyono (SBY) yang beralamat: <http://www.presidensby.info>. Pemuda yang berprofesi sebagai tekhnisi komputer tersebut ditangkap di tempat kerjanya di Warnet Surya Com beralamat di Jalan Letjend Suprapto, Kelurahan Kebonsari, Kecamatan Sumbersari. Menurut pengakuaan pemilik warnet Adi Kurniawan, salah satu pegawainya tersebut terakhir terlihat bekerja pada Jumat 25 Januari 2013, malam. “Sejak itu Wildan tidak pernah masuk bekerja dan rekan kerjanya pun tidak ada yang mengetahui keberadaanya,” kata Adi. Dalam akun Facebook Wildan disebutkan, dia mengaku bekerja Internet Security Systems dan pernah belajar soal teknologi internet di Google.com. Situs <http://www.presidensby.info> itu sebelumnya diretas Wildan pada Rabu 9 Januari 2013.  Dia meninggalkan jejak dengan menuliskan diri sebagai Jember Hacker Team. Berdasarkan pelacakan yang dilakukan Id-SIRTII, lokasi IP Address dan DNS pelaku berasal dari Texas, Amerika Serikat. Namun setelah ditelusuri, alamat pelaku di Indonesia tepatnya di Jember. Sementara Kepala Seksi Pidana Umum Kejari Jember Mujiarto mengatakan, sampai saat ini berkas penyidikan dari Mabes Polri memang masih belum turun.

Menurut Undang-Undang ITE

 Undang – undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik.

Undang – undang nomor 36 tahun 1999 tentang telekomunikasi

Sumber :

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

<http://ginanjar1.blogspot.co.id/2013/09/asas-asas-cyber-law.html>

<http://ginanjar1.blogspot.co.id/2013/09/perkembangan-cyber-law.html>

<http://mesamanth4.blogspot.co.id/2015/04/kasus-illegal-acces.html>

1. **Kasus Profokasi Melalui Internet**

JAKARTA, KOMPAS.com

— Berpikir panjanglah sebelum memasang status provokasi di media sosial. Feri Yanto, sopir [Blue Bird](http://indeks.kompas.com/tag/blue.bird) yang mengajak sesama sopir untuk membawa senjata saat demo, divonis 1,5 tahun oleh majelis hakim Pengadilan Negeri Jakarta Selatan.

Feri menuturkan, semua bermula saat ia diundang percakapan grup WhatsApp oleh mantan rekannya di [Blue Bird](http://indeks.kompas.com/tag/blue.bird) yang bernama Wendy.

Wendy yang katanya sukses menjadi sopir perusahaan transportasi *online* terus-terusan mengajak Feri untuk segera pindah. Feri yang bersikukuh bahwa ia akan bertahan di [Blue Bird](http://indeks.kompas.com/tag/blue.bird) semakin dipojokkan dan dihina.

Terpancing hinaan dan tantangan para sopir transportasi *online*, Feri menulis di akun [Facebook](http://indeks.kompas.com/tag/facebook)-nya sebuah pesan provokatif pada Minggu (20/3/2016).

Dia juga menuliskan ancaman bagi para sopir dan pengguna transportasi *online* Grab Car dan [Uber](http://indeks.kompas.com/tag/uber). Selain itu, Feri mengunggah foto senjata tajam berupa celurit dan pedang.

Namun, pada saat unjuk rasa pada 22 Maret 2016, Feri bekerja seperti biasa dan tidak terlibat sama sekali dalam pengerahan massa demonstrasi.

Sorenya, Feri diminta kembali ke pul-nya di [Bintaro](http://indeks.kompas.com/tag/bintaro), [Tangerang](http://indeks.kompas.com/tag/tangerang) Selatan, karena dipanggil oleh manajemen. Ia diminta untuk menghapus semua status tersebut.

Feri kemudian menghapus status di [Facebook](http://indeks.kompas.com/tag/facebook), termasuk percakapan di WhatsApp dan [Facebook](http://indeks.kompas.com/tag/facebook) Messenger dengan pesan terakhir dari salah satu anggota grup yang menyatakan Feri akan dipenjara dan keluarganya akan sengsara.

Pada 23 Maret, Feri ditangkap Subdit Cyber Crime Direktorat Reserse Kriminal Khusus Polda Metro Jaya dan diproses hingga kejaksaan menuntutnya dua tahun penjara.

Setelah hakim mengetuk palu, Feri masih bersumpah bahwa ia tak ada maksud sedikit pun untuk membuat rusuh. Ia sempat menitikkan air mata karena kaget hakim menyatakan ia bertanggung jawab terhadap aksi unjuk rasa sopir taksi pada Maret lalu.

“Saya harus dipisahkan dengan istri dan enam anak saya. Sekarang juga saya tidak bisa menafkahi mereka,” ujarnya, Kamis.

Kuasa hukum Feri, Riesqi Rahmadiansyah, mengatakan, setelah mendengar putusan, ia langsung diminta oleh para pihak yang kala itu mengoordinasi unjuk rasa untuk mengajukan banding.

Sebab, dakwaan Feri dianggap sebagai sikap untuk membungkam aspirasi para sopir taksi konvensional. Apa yang didakwakan kepada Feri dianggap berlebihan.

“Hari Selasa saya akan ajukan surat kuasa ke Feri untuk mengajukan memori banding,” ujar Riesqi saat dihubungi.

Hakim Pengadilan Negeri Jakarta Selatan Amet Khusaeri memutuskan Feri telah melanggar Pasal 28 Ayat (2) *jo* 45 Ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dia juga didakwa melanggar Pasal 160 KUHP tentang Penghasutan.

sumber :

<http://megapolitan.kompas.com/read/2016/08/12/09502471/status.facebook.yang.mengantar.sopir.blue.bird.divonis.1.5.tahun>

1. Masuk pasal berapa yang dicontohkan pada video di Youtube tersebut?
2. Penyebaran virus dan worm

**UU ITE dan Pasal Mengenai Virus**

Virus komputer dibuat oleh manusia dan disebarkan/diproduksi oleh mesin komputer. Bila aparat penegak hukum mampu untuk menangkap si pembuat virus dan membuktikan kejahatannya, maka pasal 32 ayat 1, pasal 33 dan pasal 36 (mengakibatkan kerugian) dapat digunakan untuk menjerat si pembuat virus. Tentunya, Hakim dalam memutuskan perkara perlu mempertimbangkan tingkat gangguan/akibat yang timbul dari jenis virus yang disebarkan.  
Virus dapat diklasifikasikan yaitu :

a.    **Tidak berbahaya**. Virus ini menyebabkan berkurangnya ruang disk untuk menyimpan data sebagai akibat dari perkembangbiakannya.

b.    **Agak berbahaya**. Virus ini menyebabkan ruang disk penuh dan mengurangi fungsi lainnya seperti kecepatan proses.

c.    **Berbahaya**. Virus ini dapat mengakibatkan kerusakan atau gangguan yang parah termasuk kerusakan data dan sistem elektronik yang diselenggarakan.

Meskipun seseorang bukan sebagai pembuat virus, tetapi dia dapat memanfaatkan virus komputer untuk merusak informasi elektronik dan/atau dokumen elektronik milik orang lain. Jika memang ada unsur kesengajaan untuk melakukan kejahatan seperti pada motif ini, maka terhadap si pelaku dapat dijerat dengan pasal 32 ayat 1, Pasal 33 dan pasal 36 UU ITE.

Pada kasus lain, seseorang misalnya si A tanpa sengaja/tidak mengetahui misalnya isi flash disk yang dimilikinya mengandung virus (sudah dicek dengan program antivirus), lalu memakai flash disk itu di komputer milik si B dan atas **seijin** si B lalu terjadi pengrusakan data oleh virus maka si A tidak dapat dijerat dengan pasal 32 ayat 1, pasal 33 dan pasal 36 UU ITE.

Jadi, meskipun virus diproduksi oleh mesin komputer, tetapi ada orang di balik penyebaran virus komputer, bisa sebagai pembuat virus atau penyebar virus dengan sengaja untuk merugikan orang lain. Mesin komputer yang memproduksi virus komputer hanya sebagai alat bantu untuk melaksanakan pembuatan dan/atau penyebaran virus, bukan pelaku kejahatan.

**Pasal 33**

*“Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya”.*

Pada kalimat awal sudah jelas bahwa setiap orang yang menunjukkan bahwa semua orang tanpa terkecuali dilarang melakukan pelanggaran melawan hukum melakukan tindakan apa pun yang berakibat terganggunya sistem elektronik atau mengakibatkan tidak bekerja sebagaimana mestinya akan mendapat sangsi sesuai dengan pasal tersebut. Pelanggaran yang dimaksud dalam pasal tersebut bisa berupa virus dan worm komputer. Sebagaimana telah kita ketahui bersama virus, worm dan jenis malware lainnya dapat mengganggu sistem elektronik menjadi tidak bekerja sebagaimana mestinya, jelas ini termasuk sebuah pelanggaran yang tertera pada pasal [33.](https://www.blogger.com/blogger.g?blogID=4528116497023376055)

Ada pelanggaran tentu ada pula hukuman/sangsi yang diberikan. Pelanggaran yang terjadi pada pasal 33 berkaitan dengan pasal 49 yang berisi dengan hukuman yang diberikan atas pelanggaran yang dilakukan.

**Pasal 49**

*“Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah)”.*

1. Spayware (hacking)

**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.

Di dalam UU ITE membahas masalah hacking terutama tentang akses ke komputer orang lain tanpa izin. Hal tersebut diatur dalam pasal 30 dan pasal 46 mengenai hukuman yang akan diterima. Berikut ini isi dari pasal tersebut:

Pasal 30

1.    Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

2.    Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

3.    Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan (cracking, hacking, illegal access).

Pasal 46

1.    Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

2.    Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah).

3.    Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

  Kitab Undang Undang Hukum Pidana

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

Sumber:

https://septiandankawan.blogspot.com/2012/12/uu-ite-dan-pasal-mengenai-hacking-virus.html