

## PERLINDUNGAN HUKUM BAGI PENGGUNA INTERNET TERHADAP FENOMENA HACKING DI INDONESIA

Indah Putri Ayu, Radiyati Pratiwi, Reyhan Devara D, Syeila Amelia

Fakultas Hukum Universitas Singaperbangsa Karawang

[indah.putriayu1177@gmail.com](mailto:indah.putriayu1177@gmail.com)

### ABSTRAK

Perkembangan teknologi informasi saat ini membawa dampak yang sangat besar bagi kehidupan sosial rakyat pesatnya perkembangan akses antar wilayah mengakibatkan dengan sangat sempit serta tanpa dibatasi oleh ruang dan saat menjadi dampak dari perkembangan teknologi informasi tidak selalu berdampak positif bagi kehidupan insan pengguna teknologi perkembangan ini pula dibarengi dengan perkembangan kejahatan tersebut dikenal dengan *cybercrime* atau kejahatan dunia maya. Kejahatan pada dunia maya terjadi karena akibat negatif dari perkembangan teknologi banyak sekali modus kejahatan yang terjadi pada dunia maya berdampak di kehidupan insan di dalamnya dunia nyata menjadi kewajiban hukum pemerintah negara untuk melindungi setiap rakyat negara perbuatan yang dapat merugikan hak warganya salah satunya adalah kejahatan itu terjadi pada dunia maya yang sering menyebabkan kerugian materil serta non kerugian untuk penggunaannya dalam mengatasi persoalan tadi pemerintah sudah memberlakukan UU No. 11 Tahun 2008 ihwal isu serta transaksi elektronika diharapkan bisa menyampaikan proteksi hukum bagi rakyat yang menggunakan teknologi tersebut dan dapat memberikan rasa aman bagi yang memakai teknologi informasi dalam beraktifitas di dunia maya.

**Kata Kunci:** Hukum Proteksi, Korban, Kejahatan Siber

### ABSTRACT

*The development of information technology today has a very large impact on the social life of the people, the rapid development of access between regions results in a very narrow and unrestricted space and when it is the impact of the development of information technology does not always have a positive impact on the lives of people who use technology, this development is also accompanied by the development of these crimes, known as cybercrime or cybercrime. Crime in cyberspace occurs because of the negative consequences of technological developments, there are many modes of crime that occur in cyberspace, impacting people's lives, in the real world, it is the legal obligation of the state government to protect every citizen of the country, an act that can harm the rights of its citizens, one of which is that crime occurs in cyberspace, which often causes material and non-loss losses for its users in overcoming the problem of the government has enacted Law No. 11 of 2008 regarding electronic issues and transactions is expected to convey legal protection for the people who use the technology and can provide a sense of security for those who use information technology in their activities in cyberspace.*

**Keywords:** Protection Law, Victims, Cybercrime

# PERLINDUNGAN HUKUM BAGI PENGGUNA INTERNET TERHADAP FENOMENA HACKING DI INDONESIA

## A. PENDAHULUAN

Kemajuan teknologi dan penerapannya selalu membawa implikasi yang beragam, baik bagi tatanan kehidupan sosial, bagi perkembangan dunia usaha, maupun bagi perkembangan nilai-nilai moral, etika, dan hukum. Perkembangan ilmu pengetahuan dan teknologi (iptek) yang cukup pesat sekarang ini sudah menjadi realita sehari-hari bahkan merupakan tuntutan masyarakat yang tidak dapat ditawar lagi. Tujuan utama dari pengembangan ilmu pengetahuan dan teknologi adalah untuk menjadikan masa depan kehidupan manusia lebih baik, lebih mudah, lebih murah, lebih cepat dan lebih aman. Perkembangan ilmu pengetahuan dan teknologi khususnya teknologi informasi seperti internet sangat membantu setiap orang untuk mencapai tujuan hidupnya dalam waktu yang singkat. Selain banyak aspek positif yang diambil dari kemajuan teknologi informasi dan transaksi komunikasi elektronik, perkembangan internet yang pesat juga menimbulkan pro dan kontra.

Penggunaan internet di Indonesia baru sebatas hiburan dan percobaan, memang setiap harinya begitu banyak orang yang *log-in* ke internet. Internet pada dasarnya digunakan untuk meningkatkan dan mempercepat proses serta memperlebar jaringan bisnis, sebagai wahana ilmiah untuk mencapai referensi berbagai perpustakaan di seluruh dunia. Namun orang Indonesia secara moral belum siap menghadapi teknologi baru ini.<sup>1</sup> Teknologi selain membawa keuntungan berupa semakin dipermudahnya hidup manusia, juga membawa kerugian-kerugian berupa semakin dipermudahnya penjahat melakukan kejahatannya. Teknologi juga memberi pengaruh yang signifikan dalam pemahaman mengenai kejahatan terutama terhadap aliran-aliran kriminologi yang menitik beratkan pada faktor manusia, baik secara lahir maupun psikologis.<sup>2</sup>

Dalam proses *hacking* terdapat kode etik yang menjadi patokan bagi para calon *hacker* maupun *hacker* profesional. Kode etik itu adalah sebagai berikut:

1. Akses ke komputer atau apapun yang dapat mengajari anda bagaimana dunia

---

<sup>1</sup> Utoyo Masudi, *Kejahatan Komputer Melalui Jaringan Internet Di Indonesia*, makalah pada seminar rutin STIMIK-MDP, Palembang, 1 November 2003, hal.13.

<sup>2</sup> *Ibid*, hal. 2.

## PERLINDUNGAN HUKUM BAGI PENGGUNA INTERNET TERHADAP FENOMENA HACKING DI INDONESIA

- bekerja haruslah tidak terbatas.
2. Semua informasi haruslah gratis (bebas)
  3. Jangan pernah percaya kepada otoritas
  4. *Hackers* atau siapapun ahruslah dihargai dengan kemampuan *hacking*-nya, bukan dikarenakan bagus criteria seperti tingaktan, umur dan posisi
  5. Kita dapat membuat keindahan dengan komputer
  6. Komputer dapat membuat hidup kita lebih baik
  7. Seperti lampu 'Aladdin', kita dapat membuat apapun dalam genggaman.<sup>3</sup>

Fenomena tindak pidana teknologi informasi merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional. Penetrasi internet yang begitu besar apabila tidak dipergunakan dengan bijak maka akan melahirkan kejahatan di dunia maya atau yang diistilahkan dengan kejahatan siber atau *cybercrime*. Pada perkembangannya dalam *cybercrime* sendiri kemudian menimbulkan istilahistilah baru bagi para pelakunya. Mereka yang suka “memainkan” internet, menjelajah ke situs internet orang lain disebut “*Hacker*” dan perbuatannya disebut “*Hacking*”. Apabila si hacker yang menyusup dan menyelundup ke situs orang lain itu dan merusak disebut sebagai “*Cracker*”. “*Hacker*” yang menjelajah berbagai situs dan “mengintip” data, tetapi tidak merusak sistem komputer, situs-situs orang atau lembaga lain disebut “*Hektivism*”. Dunia maya (*cyberspace*) saat ini ternyata rentan terhadap perilaku kriminal. Sebagai contoh kasus Bjorka yang diduga telah meretas data pelanggan Indihome, data registrasi SIM Card, data KPU RI, dan sejumlah dokumen surat menyurat milik Jokowi, termasuk surat yang dikirim oleh Badan Intelijen Negara (BIN) (Tribunnews.com).

Tindak pidana peretasan adalah salah satu bagian dari kejahatan mayantara atau *cybercrime* yang muncul akibat adanya kemajuan teknologi. Hal ini telah diatur dalam pasal 30 ayat (1), (2), (3) Undang-Undang 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang selanjutnya

---

<sup>3</sup> <http://ezine.echo.or.id/ezinel/all%20aboutz%20hacking%20h3d87%20a.k.a%20moby.txt>. All aboutz hacking,

## **PERLINDUNGAN HUKUM BAGI PENGGUNA INTERNET TERHADAP FENOMENA HACKING DI INDONESIA**

disebut dengan UU ITE. Dan, untuk sanksi pidananya telah diatur dalam pasal 46 ayat (1),(2),(3) UU ITE. Selain mendatangkan keuntungan atau nilai-nilai positif, teknologi juga mengandung muatan yang merugikan kehidupan bangsa (Wahid & Labib, 2005).

Berdasarkan uraian latar belakang di atas, maka dapat dirumuskan rumusan masalahnya antara lain sebagai berikut: Pertama, Bagaimana Perspektif Hukum Terhadap Fenomena *Hacking* Yang Dilakukan Oleh Bjorka Menurut Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik? Kedua, Bagaimana Upaya Pemerintah Dalam Menanggulangi Fenomena *Cybercrime* Di Masa Yang Akan Datang?

### **B. METODE PENELITIAN**

Metode penulisan yaitu yuridis normatif dengan menggunakan pendekatan peraturan perundang-undangan dan pendekatan konsep berdasarkan Undang-Undang atau pun peraturan tertulis lainnya yang terkat dengan isu yang di paparkan. Adapun untuk penyusunan penelitian ini ada berapa yang diperoleh dari sumber bahan hukumnya yakni; Sumber bahan hukum primer yang diperoleh secara langsung berupa Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, selain itu juga konsep cyber crime menurut para ahli, dan setelah bahan hukum terkumpul dilakukan analisis secara deduktif dan diperoleh hasil.

### **C. PEMBAHASAN (HASIL PENELITIAN) DAN ANALISIS**

#### **1. Perspektif Hukum Terhadap Fenomena *Hacking* yang Dilakukan oleh Bjorka Menurut Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik**

Banyaknya peretasan tersebut menjadi pusat perhatian dunia internasional. Saat International Information Industry Congress (IIC) tahun 2000 di Kanada telah dirumuskan mengenai kewaspadaan perkembangan *cybercrime* yang dapat merusak sistem dan data teknologi negara dan perusahaan. Tindakan peretasan terhadap media sosial tergolong ke

## PERLINDUNGAN HUKUM BAGI PENGGUNA INTERNET TERHADAP FENOMENA HACKING DI INDONESIA

dalam tindakan kejahatan baru dibanding tingkat kejahatan konvensional lainnya. Penegakan terhadap peretasan di Indonesia masih belum mencerminkan penegakan hukum yang efektif meski Indonesia telah memiliki UU sebagai dasar aturannya.

Peretasan ialah salah satu bagian dari kejahatan mayantara atau *cybercrime* yang muncul akibat adanya kemajuan teknologi. Hal ini telah diatur dalam pasal 30 ayat (1), (2), (3) Undang-Undang No. 19 Tahun 2016 perubahan atas Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang selanjutnya disebut dengan UUIITE. Dan, untuk sanksi pidananya telah diatur dalam pasal 46 ayat (1), ayat (2), ayat (3) UU ITE.

Selain mendatangkan keuntungan atau nilai-nilai positif, teknologi juga mengandung muatan yang merugikan kehidupan bangsa. Maraknya tindakan peretasan menimbulkan banyak kerugian berupa materiil dan nonmateriil yang diderita oleh korban itu sendiri. Peretasan ini juga tidak hanya dilakukan pada situs web tetapi juga pada akun media sosial milik perseorangan. Dari sekian banyak sisi gelap dari kemajuan teknologi, teknologi masih menyimpan banyak keuntungan positif seperti adanya email, *e-commerce*, *internet banking*, dan hal lain semacamnya.

Kejahatan mayantara (*cybercrime*) yang timbul akibat adanya kemajuan teknologi yang begitu pesat banyak mengakibatkan dampak negatif dan positif dari adanya teknologi tersebut. Dampak positif dapat berupa adanya e-mail, internet banking, serta hal-hal lain. Namun, perkembangan ini juga membawa pengaruh negatif seperti adanya tindak pidana peretasan (*hacking*) yang dilakukan guna untuk memperoleh informasi atau data-data penting lainnya. Dalam perlindungan hukum terhadap korban *cybercrime* secara mendasar ada dua model yaitu model hak-hak prosedural dan model pelayanan.<sup>4</sup>

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang merupakan piranti hukum terbesar yang diharapkan dapat mengakomodir segala jenis pelanggaran dalam bidang IT. Disamping terdapat perlindungan hukum, disana juga terdapat ancaman sanksi pidana atas pelanggaran yang dilakukan.

---

<sup>4</sup> Muladi dan Barda Nawawi Arif, Bunga Rampai Hukum Pidana, Alumni, Bandung, 1992, Hal. 79

## **PERLINDUNGAN HUKUM BAGI PENGGUNA INTERNET TERHADAP FENOMENA HACKING DI INDONESIA**

Tindak pidana peretasan yang diatur dalam pasal 30 ayat (1), (2), dan (3) mengandung unsur sebagai berikut. Pasal 30 ayat (1) UU ITE: “setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun”. Dalam pasal ini sudah jelas tertera unsur setiap orang, unsur dengan sengaja dan tanpa hak melawan hukum, unsur mengakses komputer dan/ atau sistem elektronik milik orang lain, serta unsur dengan cara apapun.

Ketentuan yang secara khusus mengatur mengenai tindak pidana peretasan telah termuat dalam pasal 30 ayat (1), ayat (2), dan ayat (3) UU ITE. Pasal ini menjelaskan bahwa setiap orang yang mencoba masuk atau mengakses sistem elektronik milik orang lain dengan cara apapun dengan sengaja dan tanpa hak melawan hukum. Pasal ini berkaitan langsung dengan pasal 46 ayat (1), ayat (2), dan ayat (3) UU ITE yang mengatur mengenai sanksi pidana atas pelanggaran yang tercantum dalam pasal 30 yang menyebutkan bahwa setiap orang dilarang secara tegas masuk kedalam sistem elektronik milik orang lain yang bersifat privasi atau pribadi. Sanksi pidanayang dapat menjerat pelaku peretasan tersebut telah diatur secara jelas dalam pasal 46 ayat 1 yakni “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). Pasal 30 ayat (2) UU ITE: “setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/ atau dokumen elektronik”.

Pemerintah dalam melakukan upaya menanggulangi kejahatan mayantara dengan skala nasional telah menerapkan peraturan Perundang-Undangan yang mengatur secara khusus mengenai IT. Kejahatan yang tanpa mengenal batas ini bisa saja sangat membahayakan jika tidak ditanggulangi dan tidak memiliki payung hukum yang kuat untuk mengakomodirnya.

### **2. Upaya Pemerintah Dalam Menanggulangi Fenomena *Cybercrime* Di Masa Yang Akan Datang**

Kebijakan dalam perundang-undangan mutlak diperlukan oleh para penegak hukum dan pemerintah untuk menaggulangi dan menindak pelaku kejahatan, sama halnya dengan

## PERLINDUNGAN HUKUM BAGI PENGGUNA INTERNET TERHADAP FENOMENA HACKING DI INDONESIA

tindak kejahatan mayantara (*cybercrime*), tentunya jenis hukum perundang-undangan haruslah sesuai dengan jenis kejahatan dan cara untuk mengungkap kasus kejahatan dunia maya. Maka dari itu sejak tahun 2008 pemerintah republik Indonesia sudah berkoitmen untuk memerangi kejahatan dunia maya.

Secara terminologi kebijakan publik (*public policy*) itu ternyata banyak sekali, tergantung dari sudut mana kita mengartikanya Easton memberikan definisi kebijakan publik sebagai *the authoritative allocation of values for whole society* atau sebagai pengalokasian nilai- nilai secara paksa kepada seluruh anggota masyarakat. Laswell dan Kaplan juga mengartikan kebijakan publik sebagai *a projected program of goal, value, and practice* atau sesuatu program pencapaian tujuan, nilai-nilai dalam praktek-praktek yang terarah. Pada sub bab ini akan dijelaskan pendekatan-pendekatan hukum apa saja yang telah dilakukan oleh pemerintah Indonesia dalam menaggulangi kejahatan *cybercrime* Dalam rangka menaggulangi kejahatan diperlukan strategi yang mantap dari Negara dan masyarakat, dan harus dilakukan dengan cara bersama-sama secara simultan.

Upaya untunk menghadirkan suatu perangkat hukum yang sesuai dengan perkembangan dunia informasi dan telekomunikasi menjadi sesuatu yang tidak bisa ditwartawar lagi. Pemerintah Indonesia melalui Kementrian Infromasi Dan Komunikasi (KOMINFO) yang bekerja dengan pihak *stakeholder* dan universitas berupaya untuk mewujudkan asa itu. Akhirnya melalui pembahasan yang begitu “alot”, sebuah undangundang yang secara khusus menyoal dan membahas permasalahan informasi dan transaksi elektronik diundangkan pada 21 april 2008 yang kemudian dikenal dengan Undang-Undang 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik .

Pada hakikatnya pemanfaatan teknologi informasi, media dan komunikasi telah mengubah perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia tanpa batas (*borderless*) dan telah menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi informasi kini telah menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan.

## PERLINDUNGAN HUKUM BAGI PENGGUNA INTERNET TERHADAP FENOMENA HACKING DI INDONESIA

Kemajuan, dan peradaban manusia. Sekaligus juga menjadi sarana efektif perbuatan melawan hukum. Lahirnya rezim hukum baru (UU ITE) yang dikenal dengan hukum telematika dapat dikatakan sebagai sebuah respon positif. Hukum telematika atau cyber law, secara internasional digunakan istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi.

Demikian pula, hukum telematika yang perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*) dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi, baik dalam lingkup lokal maupun global (internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang sering kali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi dan transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Pemerintah dalam melakukan upaya menanggulangi kejahatan mayantara dengan skala nasional telah menerapkan peraturan Perundang-Undangan yang mengatur secara khusus mengenai IT. Kejahatan yang tanpa mengenal batas ini bisa saja sangat membahayakan jika tidak ditanggulangi dan tidak memiliki payung hukum yang kuat untuk mengakomodirnya. Upaya penanggulangan kejahatan tersebut dapat berupa upaya preventif dan upaya represif.

- a. Upaya preventif, Upaya ini merupakan upaya pencegahan yang dilakukan guna mencegah timbulnya suatu kejahatan didalam lingkup masyarakat. Beberapa hal yang dapat dilakukan guna mencegah terjadinya suatu kejahatan adalah dengan melakukan edukasi terhadap masarakat, melakukan pemblokiran, membentuk Badan Siber dan Sandi Negara (BSSN).
- b. Upaya represif, Upaya ini merupakan salah satu upaya yang bersifat konsepsional, dimana upaya ini dilakukan setelah terjadinya suatu kejahatan. Upaya ini bertujuan untuk menindak pelaku kejahatan seperti penjatuhan sanksi atau penjatuhan pidana sesuai dengan pelanggaran yang telah dilakukan.

## PERLINDUNGAN HUKUM BAGI PENGGUNA INTERNET TERHADAP FENOMENA HACKING DI INDONESIA

Dalam memberikan perlindungan hukum terhadap korban *cybercrime* aparat penegak hukum khususnya pihak kepolisian telah melakukan berbagai cara dalam mengatasi maraknya kejahatan yang terjadi di dunia maya salah satunya sosialisasi kepada masyarakat pengguna teknologi dan bagi masyarakat yang pernah menjadi korban *cybercrime* dapat melaporkan penipuan yang dialami dengan mengirim laporan ke alamat surel yakni *cybercrime@polri.go.id*.<sup>5</sup>

### D. PENUTUP

Fenomena kemunculan Bjorka yang membocorkan data pribadi warga, termasuk 105 juta data kependudukan KPU pada 6 September 2022 serta data dua menteri Kabinet Indonesia Maju, menunjukkan lemahnya sistem keamanan data pribadi yang seharusnya dilindungi negara. Terlepas dari motif pelaku, tindakan tersebut merupakan perbuatan ilegal yang melanggar Pasal 30 UU ITE dan diancam sanksi pidana sebagaimana diatur dalam Pasal 46 UU ITE, dengan ancaman penjara hingga 8 tahun dan denda hingga 800 juta rupiah. Peristiwa ini menjadi peringatan serius bagi pemerintah untuk memperkuat keamanan siber nasional, karena kebocoran data berpotensi disalahgunakan oleh pihak tidak bertanggung jawab dan menimbulkan keresahan di masyarakat. Oleh karena itu, di era digital saat ini, pemerintah dituntut untuk meningkatkan perlindungan teknologi dan informasi agar masyarakat dapat mengikuti perkembangan zaman tanpa rasa cemas terhadap keamanan data pribadinya.

### DAFTAR PUSTAKA

- Santoyo, 2008, Penegakan Hukum di Indonesia, Jurnal Hukum, Program Studi Ilmu Hukum Fakultas Hukum Universitas Jenderal Soedirman Purwokerto, Volume 8, Nomor 3.
- Kerta Negara, 2017, "Vidio: Bandar Judi Online Diburu Ke Jakarta" <http://www.balipost.com>. Diakses tanggal 7 April 2018.
- Andi Hamzah, 1990, Aspek-aspek Pidana di Bidang Komputer, Sinar Grafika, Jakarta. Arif Gosita, 2004,

---

<sup>5</sup> Jakarta, Tribun-Timur.Com.

## **PERLINDUNGAN HUKUM BAGI PENGGUNA INTERNET TERHADAP FENOMENA HACKING DI INDONESIA**

- Masalah Korban Kejahata, PT Bhuana Ilmu Populer, Jakarta Barda Nawawi Arief, 2000,
- Perlindungan HAM dan Korban dalam Pembaharuan Hukum, Citra Aditya Bakti, Bandung. Dikdik M Arief Mansyur dan Elisatris Gultom, 2008,
- Urgensi Perlindungan Korban Kejahatan, PT Raja Grafindo Persada, Jakarta. J.E Sahetapy, 1987, Viktimologi Sebuah Bunga Rampai, cetakan pertama, Pustaka Sinar Harapan, Jakarta.
- Kitab Undang-Undang Hukum Pidana (KUHP)  
Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik
- [http://repo.unsrat.ac.id/235/1/Kejahatan\\_Hacking\\_Melalui\\_Jaringan\\_Internet\\_Di\\_Indonesia.pdf](http://repo.unsrat.ac.id/235/1/Kejahatan_Hacking_Melalui_Jaringan_Internet_Di_Indonesia.pdf). Diakses pada 27 Desember 2022.
- <http://ezine.echo.or.id/ezinel/all%20aboutz%20hacking%20h3d87%20a.k.a%20moby.txt>.  
All aboutz hacking.