

MAKALAH
CYBERCRIME (ILLEGAL CONTENT)



TUGAS KULIAH

Diajukan untuk memenuhi tugas mata kuliah Etika Profesi Teknologi Informasi
dan Komunikasi

Disusun oleh :

- | | |
|----------------------------|------------|
| 1. Asep Saepul Anwar | (11180600) |
| 2. Detaviani Sri Wijayanti | (11180189) |
| 3. Dini Nurdayanti | (11180116) |
| 4. Fara Dida Daniar | (11181150) |
| 5. Ikbal Amrulloh | (11180198) |
| 6. M. Dede Masrudin | (11180023) |
| 7. Rizki Ade Gunawan | (11180259) |

Kelas : 11.6B.24

https://asepsaepulanwar218.github.io/eptik_kel-3/

Program Studi Sistem Informasi Akuntansi
Fakultas Teknik dan Informatika
Universitas Bina Sarana Informatika
Jakarta
2021

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah SWT karena atas terselesaikannya Makalah Cybercrime (Illegal Content). Tujuan pembuatan makalah ini untuk memenuhi tugas mata kuliah Etika Profesi Teknologi Informasi dan Komunikasi pada Program Diploma Tiga (D.III) Universitas Bina Sarana Informatika.

Penulis menyadari bahwa dalam pembuatan makalah ini memiliki banyak kekurangan. Oleh karena itu dengan segala kerendahan hati penulis berharap pembaca dapat memaklumi atas segala kekurangan makalah ini, karena penulis hanyalah manusia biasa yang tak luput dari khilaf serta keterbatasan kemampuan penulis sehingga yakin bahwa laporan ini masih jauh dari kesempurnaan, untuk itu kami membutuhkan kritik dan saran yang bersifat membangun demi kesempurnaan dimasa yang akan datang.

Semoga laporan ini dapat bermanfaat bagi semua pihak, khususnya bagi kami, umumnya bagi rekan-rekan maupun pembaca. Akhir kata kami ucapkan terima kasih kepada para pembaca yang senantiasa mendukung dan memberikan kritik dan sarannya sehingga kami bisa memperbaiki makalah ini menjadi lebih baik.

Cikarang, 31 Mei 2021

Penulis

DAFTAR ISI

KATA PENGANTAR	ii
DAFTAR ISI	iii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	1
1.3 Maksud dan Tujuan	2
BAB II LANDASAN TEORI	3
2.1 Cybercrime.....	3
2.1.1 Jenis-jenis Cybercrime.....	4
2.2 Cyber Law	6
BAB III PEMBAHASAN	8
3.2 Pengertian Illegal Content.....	8
3.2 Contoh Kasus Illegal Content	8
3.3 Pelaku dan Peristiwa Dalam Kasus <i>Illegal contents</i>	10
3.4 Penyebab Illegal Content	11
3.5 Penanggulangan <i>Illegal content</i>	12
BAB IV PENUTUP	13
4.1 Kesimpulan	13
4.2 Saran	13
DAFTAR PUSTAKA	15

BAB I

PENDAHULUAN

1.1 Latar Belakang

Saat ini kita dapat melihat bahwa hampir seluruh kegiatan manusia mengandalkan teknologi yang menghadirkan kemudahan bagi penggunaanya berupa akses bebas yang dapat dilakukan oleh siapapun, kapanpun dan dimanapun tanpa sensor serta ditunjang dengan berbagai penawaran internet murah dari penyedia jasa layanan internet.

Internet menawarkan kepada manusia berbagai harapan dan kemudahan. Akan tetapi dibalik itu, timbul persoalan berupa kejahatan yang dinamakan cybercrime, baik sistem jaringan komputernya itu sendiri yang menjadi sasaran maupun komputer itu sendiri yang menjadi sarana untuk melakukan kejahatan. Tentunya jika kita melihat bahwa informasi itu sendiri telah menjadi komoditi maka upaya untuk melindungi asset tersebut sangat diperlukan. Salah satunya dengan melalui hukum pidana, baik dengan bersarana penal maupun non penal.

Akhir-akhir ini juga sering terjadi penyebaran hal-hal yang tidak teruji kebenaran akan faktanya yang tersebar bebas di internet, baik itu dalam bentuk foto, video maupun berita-berita hoax. Dalam hal ini tentu saja mendatangkan kerugian bagi pihak yang menjadi korban dalam pemberitaan yang tidak benar tersebut, seperti kita ketahui pasti pemberitaan yang di beredar merupakan berita yang sifatnya negatif. Yang menarik dari hukuman atau sanksi untuk beberapa kasus seseorang yang terlibat dalam illegal content ini ialah penyebar atau yang melakukan proses unggah saja mendapat sanksi. Sedangkan yang mengunduh tidak mendapat hukuman apapun selain hukuman moral dan perasaan bersalah setelah mengunduh file yang sangat tidak baik.

1.2 Rumusan Masalah

- a. Definisi Cybercrime, klasifikasi, serta jenis-jenisnya
- b. Pengertian Illegal Content

- c. Contoh kasus yang menyangkut Illegal Content
- d. Siapa saja yang termasuk pelaku dan peristiwa dalam Illegal Content
- e. Penyebab terjadinya Illegal Content
- f. Bagaimana upaya penanggulangan tindakan *Illegal Content*

1.2 Maksud dan Tujuan

Makalah ini dibuat dengan maksud untuk membeikan informasi mengenai kejahatan komputer khususnya *illegal content*. Setelah mempelajari makalah ini, diharapkan agar para pembaca dan penulis mampu memahami tentang pengertian illegal content, kasus illegal content, pihak-pihak yang termasuk dalam *illegal content*, penyebab terjadinya *illegal content*, serta upaya penanggulangannya.

Sedangkan tujuan penulisan makalah ini adalah untuk memenuhi tugas Mata Kuliah Etika Profesi & Komunikasi (EPTIK) pada Jurusan Sistem Informasi Akuntansi Semester VI di Universitas Bina Sarana Informatika (UBSI) Kampus Cikarang.

BAB II

LANDASAN TEORI

2.1 Cybercrime

Cyber crime adalah suatu aktivitas kejahatan di dunia maya dengan memanfaatkan jaringan komputer sebagai alat dan jaringan internet sebagai medianya.

- Dalam arti luas, pengertian *cyber crime* adalah semua tindakan ilegal yang dilakukan melalui jaringan komputer dan *internet* untuk mendapatkan keuntungan dengan merugikan pihak lain.
- Dalam arti sempit, pengertian *cybercrime* adalah semua tindakan ilegal yang ditujukan untuk menyerang sistem keamanan komputer dan data yang diproses oleh suatu sistem komputer.

Cyber crime atau kejahatan dunia maya dapat dilakukan dengan berbagai cara dan beragam tujuan. Kejahatan dunia maya ini umumnya dilakukan oleh pihak-pihak yang mengerti dan menguasai bidang teknologi informasi. Kejahatan dunia maya ini mulai muncul sejak tahun 1988 yang pada masa itu disebut dengan sebutan *Cyber Attack*. Pelaku *cybercrime* pada saat itu menciptakan *worm/virus* untuk menyerang komputer yang mengakibatkan sekitar 10% komputer di dunia yang terkoneksi ke internet mengalami mati total.

Cybercrime memiliki karakteristik sebagai berikut :

1. Ruang lingkup kejahatan
2. Sifat kejahatan
3. Pelaku kejahatan
4. Modus kejahatan
5. Jenis kerugian yang ditimbulkan

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

1. *Cyberpiracy*

Penggunaan teknologi komputer untuk mencetak ulang *software* atau informasi, lalu mendistribusikan informasi atau *software* tersebut lewat teknologi komputer.

2. *Cybertrespass*

Penggunaan teknologi komputer untuk meningkatkan akses pada *system computer* suatu organisasi atau indifidu.

3. *Cybervandalism*

Penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi elektronik, dan menghancurkan data dikomputer.

2.1.1 Jenis-jenis Cybercrime

Secara umum, jenis-jenis *cyber crime* adalah sebagai berikut :

a. Akses Ilegal (*Unauthorized Access*)

Membuka atau masuk ke akun orang lain tanpa ijin dan dengan sengaja merupakan suatu tindakan kejahatan di dunia maya. Akun yang telah dibobol pelaku sangat mungkin membuat pemiliknya mengalami kerugian, misalnya :

- Membuat pemilik akun kehilangan data penting
- Menggunakan akun untuk aksi kejahatan, misalnya menipu orang lain dengan memakai nama pemilik akun

b. Menyebarkan Konten Ilegal (*Illegal Contents*)

Konten ilegal adalah konten yang didalamnya terdapat informasi atau data yang tidak etis, tidak benar, atau melanggar hukum. Ada banyak sekali jenis

konten ilegal yang disebarkan di *internet*. Namun, yang paling sering disebarkan adalah berita HOAX dan juga konten yang mengandung unsur porno.

c. *Hacking* dan *Cracking*

Sebenarnya *hacking* mengacu pada kegiatan mempelajari sistem komputer secara mendetail dan meningkatkan kemampuan komputer. Namun, banyak *hacker* yang menyalah gunakan kemampuannya dengan melakukan kejahatan di dunia maya.

Sedangkan *cracking* adalah tindakan pembajakan terhadap hak milik orang lain. Misalnya pembajakan akun, pembajakan situs *website*, penyebaran *virus*, *probing*, dan lainnya.

d. Pemalsuan Data (*Data Forgery*)

Ini merupakan tindak kejahatan dunia maya dengan memalsukan data pada dokumen penting yang disimpan sebagai *scriptles document* di *internet*. Salah satu praktik pemalsuan data ini misalnya pemalsuan dokumen pada situs *e-commerce* yang dibuat seolah-olah terjadi *typo* atau salah ketik sehingga menguntungkan pelakunya.

e. Penyalahgunaan Kartu Kredit (*Carding*)

Carding adalah bentuk kejahatan di dunia maya dimana pelakunya berbelanja dengan menggunakan nomor dan identitas kartu kredit milik orang lain. Praktik *carding* ini sangat merugikan para pemilik kartu kredit yang dicuri datanya. Itulah sebabnya saat ini semua negara sangat ketat dalam mengawasi transaksi kartu kredit, terutama yang melibatkan transaksi luar negeri

f. Pencurian Data (*Data Theft*)

Ini adalah aktivitas mencuri data dari sistem komputer secara ilegal, baik untuk kepentingan sendiri atau dijual kepada pihak lain. Tindakan pencurian data ini sering berujung pada kejahatan penipuan (*fraud*) secara online.

g. Memata-matai (*Cyber Espionage*)

Ini adalah kejahatan di dunia maya yang memanfaatkan jaringan *internet* untuk masuk ke sistem jaringan komputer pihak lain untuk memata-matai.

h. *Cyber Squatting*

Tindak kejahatan di dunia maya dimana pelakunya mendaftarkan domain dengan nama suatu perusahaan lalu menjualnya kepada perusahaan tersebut dengan harga tinggi.

i. *Cyber Typosquatting*

Cyber crime dimana pelakunya meniru atau mengklon situs *website* pihak lain dengan tujuan untuk melakukan penipuan atau berita bohong kepada masyarakat.

2.2 Cyber Law

Cyber Law adalah hukum yang digunakan di dunia maya (*cyber*) yang diasosiasikan dengan *internet* yang isinya mengupas mengenai aspek-aspek aktivitas manusia pada saat menggunakan *internet* dan memasuki dunia maya atau *cyber* namun diartikan secara sempit kepada apa yang diaturnya. Sebab alasan perlunya *cyberlaw*, diantaranya :

1. Perkembangan teknologi yang sangat pesat, membutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi tersebut. Sayangnya, hingga saat ini banyak negara belum memiliki perundang-undangan khusus di bidang teknologi informasi, baik dalam aspek pidana maupun perdatanya
2. Permasalahan yang sering muncul adalah bagaimana menjaring berbagai kejahatan komputer dikaitkan dengan ketentuan pidana yang berlaku karena ketentuan pidana yang mengatur tentang kejahatan komputer yang berlaku saat ini masih belum lengkap
3. Banyak kasus yang membuktikan bahwa perangkat hukum di bidang TI masih lemah. Seperti contoh, masih belum ilakunya dokumen elektronik secara tegas sebagai alat bukti oleh KUHP. Hal tersebut dapat dilihat pada UU No8/1981 Pasal 184 ayat 1 bahwa undang-undang ini secara definitif membatasi alat-alat bukti hanya sebagai keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa saja. Demikian juga dengan kejahatan pornografi dalam internet, misalnya KUH Pidana pasal 282 mensyaratkan bahwa unsur pornografi dianggap kejahatan jika dilakukan di tempat umum.

4. Hingga saat ini, di negara kita ternyata belum ada pasal yang bisa digunakan untuk menjerat penjahat *cybercrime*. Untuk kasus *carding* misalnya, kepolisian baru bisa menjerat pelaku kejahatan komputer dengan pasal 363 soal pencurian karena yang dilakukan tersangka memang mencuri data kartu kredit orang lain.

BAB III

PEMBAHASAN

3.2 Pengertian Illegal Content

Illegal Contents adalah 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. Dalam artian sederhana, *illegal content* merupakan kegiatan menyebarkan seperti mengunggah dan menulis hal yang salah atau dilarang yang dapat merugikan orang lain.

Sebagai contohnya, 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.

Illegal content menurut pengertian diatas dapat disederhanakan pengertiannya menjadi : kegiatan menyebarkan (mengunggah,menulis) hal yang salah atau diarang / dapat merugikan orang lain.

3.2 Contoh Kasus Illegal Content

a. *Cyberporn*

Cyberporn merupakan kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan dan menyebarkan material yang berbau pornografi, cabul dan mengekspos hal-hal yang tidak pantas. *Cyberporn* telah menjadi salah satu dalang rusaknya mentalitas generasi muda bangsa. Pemerintah telah mengeluarkan beberapa undang-undang untuk mengatasi laju *cyberporn* di Indonesia, diantaranya :

- a. Pasal 281-283 Kitab Undang-undang Hukum Pidana (KUHP), melarang pornografi dalam bentuk apapun.

- b. Undang-undang nomor 36 tahun 2009 tentang telekomunikasi, pasal 5 ayat 1 dan pasal 13 ayat 1 huruf a.
- c. Undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik (UU ITE)
- d. Undang-undang nomor 44 tahun 2008 tentang pornografi.

b. *Hoax*

Hoax adalah pemalsuan berita yang dilakukan oleh oknum-oknum yang tidak bertanggung jawab dengan cara menyebarkan berita yang belum tentu kebenarannya, kemudian dipublikasikan lewat internet. Hal ini sangat merugikan pihak lain, dari banyak kasus yang terjadi para pelaku kejahatan ini susah dilacak sehingga proses hukum tidak dapat berjalan dengan baik.

Akhir-akhir ini juga sering terjadi penyebaran hal-hal yang tidak teruji kebenaran akan faktanya yang tersebar bebas di internet, baik itu dalam bentuk foto, video maupun berita-berita. Dalam hal ini tentu saja mendatangkan kerugian bagi pihak yang menjadi korban dalam pemberitaan yang tidak benar tersebut, seperti kita ketahui pasti pemberitaan yang di beredar merupakan berita yang sifatnya negatif.

Salah satu contoh nyata tentang penyebaran berita *hoax* adalah kasus kebohongan Ramaditya seorang *blogger motivator* tunanetra. Ramaditya seorang tunanetra yang pernah dua kali menjadi bintang tamu di acara yang notabene diercaya, *Kick andy* memiliki suatu kelebihan yaitu bisa mengoperasikan *computer* dengan sangat baik dan juga pandai memainkan alat musik menghebohkan dunia *internet* di akhir bulan agustus 2010 lalu. Ramaditya melakukan sebuah pengakuan yang membuat semua netter terkejut. Dia mengaku kalau semua claim selama ini atas profesinya sebagai pencipta musik – musik game online besar di Jepang itu hanyalah sebuah kebohongan publik.

Ramaditya tidak mendapatkan sanksi hukum akan tetapi karena telah melanggar kode etik profesi maka dia mendapat sanksi moral berupa celaan sesama netter dan juga pemutusan kontrak-kontrak pekerjaan *offline*. Begitulah kode etik suatu profesi berjalan apabila dilanggar maka yang telah melanggar kode etik tersebut akan tersingkir dari profesi yang sebelumnya digeluti dan membuat kepercayaan orang hilang terhadap kemampuan serta eksistensi yang dimiliki

sebelumnya. Walaupun seorang ramaditya memang benar-benar pandai mengoperasikan *computer* dan juga memang benar-benar bisa menulis di blognya akan tetapi kepercayaan publik telah hilang dikarenakan dia menyebarkan kebohongan dan juga mengakui hak cipta orang lain sebagai ciptaannya.

3.3 Pelaku dan Peristiwa Dalam Kasus *Illegal contents*

A. Pelaku

Pelaku yang menyebarkan informasi elektronik atau dokumen elektronik yang bermuatan *Illegal Content* baik perseorangan atau badan hukum. Sesuai isi Pasal 1 angka 21 UU ITE bahwa “Orang adalah orang perorangan baik warga negara Indonesia maupun warga negara asing atau badan hukum”. Keberadaan Badan Hukum diperjelas kembali dalam Pasal 52 ayat (4) UU ITE bahwa korporasi yang melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai Pasal 37 UU ITE, termasuk menyebarkan informasi elektronik atau dokumen elektronik yang bermuatan *Illegal Content* dikenakan pemberatan pidana pokok ditambah dua pertiga.

B. Peristiwa

Perbuatan penyebaran informasi elektronik atau dokumen elektronik seperti dalam Pasal 27 sampai Pasal 29 harus memenuhi unsur:

1. *Illegal Content* seperti penghinaan, pencemaran nama baik, pelanggaran kesusilaan, berita bohong, perjudian, pemerasan, pengancaman, menimbulkan rasa kebencian atau permusuhan individu, ancaman kekerasan atau menakut-nakuti secara pribadi.
2. Dengan sengaja dan tanpa hak, yakni dimaksudkan bahwa pelaku mengetahui dan menghendaki secara sadar tindakannya itu dilakukan tanpa hak. Pelaku secara sadar mengetahui dan menghendaki bahwa perbuatan “mendistribusikan” atau “mentransmisikan” atau “membuat dapat diaksesnya informasi elektronik atau dokumen elektronik” adalah memiliki muatan melanggar kesusilaan. Dan tindakannya tersebut dilakukannya tidak *legitimate interest*.

Perbuatan pelaku berkaitan *Illegal Content* dapat dikategorikan sebagai berikut:

- a) Penyebaran informasi elektronik yang bermuatan *illegal content*.
- b) Membuat dapat diakses informasi elektronik yang bermuatan *illegal content*.
- c) Memfasilitasi perbuatan penyebaran informasi elektronik, membuat dapat diaksesnya informasi elektronik yang bermuatan *illegal content* (berkaitan dengan pasal 34 UU ITE).

3.4 Penyebab Illegal Content

Seiring berkembangnya teknologi yang sangat pesat tidak selalu membuahkan hasil yang bagus apabila sumber daya manusianya tidak memiliki pengetahuan yang cukup, sehingga dapat di salah gunakan dan di manfaatkan oleh oknum yang sudah ahli dalam bidang sistem informasi dan komunikasi serta memiliki niat jahat untuk kepentingan pribadi mereka. Berikut ini adalah beberapa hal yang menyebabkan maraknya *illegal content* :

1. Pihak yang memproduksi dan yang menerima serta yang mengakses tidak terdapat aturannya.
2. Definisi kesusilaan belum ada penjelasan batasannya.
3. Pelaku *cybercrime* susah dilacak sehingga sulit di adili oleh hukum.
4. Dalam pasal perjudian *online* para penjudi tidak dikenakan pidana.
5. Dalam pasal penghinaan dan atau pencemaran nama baik pembuktian harus dilakukan dengan hati – hati karena dapat dimanfaatkan oleh oknum yang arogan.
6. Dalam pasal penyebaran berita bohong dan penghasutan melalui internet pihak yang menjadi korban adalah konsumen dan pelakunya produsen, sementara dilain pihak bisa jadi yang menjadi korban sebaliknya.
7. Dalam pasal provokasi melalui internet disebutkan informasi dan tidak dijelaskan informasinya seperti apa.

3.5 Penanggulangan *Illegal content*

Untuk menanggulangi kejahatan internet yang semakin meluas maka diperlukan suatu kesadaran dari masing-masing negara akan bahaya penyalahgunaan internet. Berikut adalah langkah ataupun cara penanggulangan *cybercrime* :

1. Menambah personil tenaga ahli ke dalam *cyberpolice*.
2. Meningkatkan pengawasan pemerintah terhadap *cybercrime*.
3. Meningkatkan pemahaman serta keahlian aparat hukum mengenai upaya pencegahan, investigasi, dan penuntutan perkara – perkara yang berhubungan dengan *illegal content*.

BAB IV

PENUTUP

4.1 Kesimpulan

Cybercrime merupakan suatu tindak kejahatan di dunia *Cyber* atau dunia maya yang sangat merugikan. *Cybercrime* merupakan akibat dari perkembangan global di bidang informasi yang di salah gunakan oleh sebagian oknum untuk melakukan tindak kejahatan.

Saat ini sudah dibentuk UU no. 11 tahun 2008 tentang Informasi dan transaksi elektronik sehingga penegasan hukum dapat dilakukan untuk mengatasi kasus-kasus *Cybercrime*. Masyarakat mulai lega dan tidak menghadapi ancaman *cybercrime* dengan jaminan kepastian hukum ini.

Disamping itu segala macam sangsi, hukum telah dipertegas dalam pasal-pasal undang-undang ini, sehingga pihak-pihak aparat penegak hukum mampu menegakkan dan menangani kasus ini dengan baik.

KUHP dan Undang-Undang lain seperti:

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 2001 tentang Hak Cipta
5. Undang-Undang Nomor 14 tahun 2001 tentang Hak Paten
6. Undang-Undang Nomor 15 tahun 2001 tentang Merk
7. Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

4.2 Saran

Berkaitan dengan *Illegal Contents* tersebut maka perlu adanya upaya untuk pencegahannya, untuk itu yang perlu diperhatikan adalah :

1. Sosialisasi hukum kepada masyarakat tentang UU ITE sehingga masyarakat bisa menempuh jalur hukum ketika menjadi korban kejahatan dalam dunia *cyber*.
2. Lakukan konfirmasi kepada perusahaan yang bersangkutan apabila Anda merasa menjadi target kejahatan *illegal content*.

DAFTAR PUSTAKA

- Akbar, M.Rizky.F, & Akbar, I. (2013). *illegal content*. Blogspot. Diakses dari <http://ilham10akbari.blogspot.com/2013/12/illegal-content.html>
- EduCyberCrime. (2013). *Contoh Kasus Illegal Content*. Cyber Crime Education. Diakses dari <https://cybercrimeedu.wordpress.com/2013/05/25/tentang-kami/>
- HASANAH, D. (2019). *MAKALAH ETIKA PROFESI TEKNOLOGI INFORMASI & KOMUNIKASI CYBERCRIME (ILLEGAL CONTENT)*. Diana Hasanah - 13.6B.01. Diakses dari <http://dianahasanahh.blogspot.com/2019/11/makalah-etika-profesi-teknologi.html>
- ILLEGAL CONTENT, DATA FORGERY & CYBER ESPIONAGE*. (n.d.). Diakses dari <https://124b23-8-eptik.weebly.com/illegal-content.html>
- Jessy. (2020). *MAKALAH ILLEGAL CONTENT EPTIK*. Wordpress. Diakses Dari <https://thismineok.wordpress.com/2020/06/10/illegal-content/>
- Kunylutfannadiyya. (2020). *Makalah Illegal Content*. Kuny Lutfannadiyya. Diakses dari <https://kunylutfannadiyya.wordpress.com/2020/06/11/makalah-illegal-content/>
- RAMDHAN, V. (n.d.). *ILEGAL CONTENTS*. Wordpress. Diakses dari <https://viraniaramdhan.wordpress.com/silabus/cyber-crime/ilegal-contents/>