2022

DIGITAL FORENSIK

(PENGERTIAN DAN KASUS)

Muhammad Syarif Hartawan M.Kom MM
Suhardjono S.Kom M.Kom
Ridwansyah, S.Kom, M.Kom
Verry Riyanto, S.Kom, M.Kom
Dr. Arman Syah Putra S.Kom MM M.Kom

ARS TRAINING

Muhammad Syarif Hartawan M.Kom MM
Suhardjono S.Kom M.Kom
Ridwansyah S.Kom M.Kom
Verry Riyanto S.Kom M.Kom
Dr. Arman Syah Putra S.Kom MM M.Kom

DIGITAL FORENSIK

(INFORMASI DAN KASUS)

2022

KATA PENGANTAR

Terima kasih kepada Allah SWT dan kedua orang tua kami atas terbit nya buku di tahun 2022 ini, dengan terbit nya buku ini di harapkan berguna untuk semua orang dalam hal riset dan penelitian di bidang data terutama di bidang digital forensik, buku ini berisikan tentang pengertian data dan kasus, diharapkan dengan ada buku-buku selanjutnya dan bisa terus berkarya agar bisa membantu dalam hal riset dan penelitian di bidang kecerdasan buatan.

Penulis

Muhammad Syarif Hartawan M.Kom MM
Suhardjono S.Kom M.Kom
Ridwansyah S.Kom M.Kom
Verry Riyanto S.Kom M.Kom
Dr. Arman Syah Putra S.Kom MM M.Kom

DAFTAR ISI

APA ITU FORENSIK DAN KASUS

1. Komputer forensik merupakan salah satu cabang ilmu forensi didalam bidang digital. Komputer forensik adalah penyelidikan yang menganalisa barang bukti yang ada secara elektornik, yang akan dipertanggung jawabkan ke sidang hukum.
2. Dampak dari komputer forensik ada 2, yaitu dampak positif dan dampak negatif. Dampak positifnya, yaitu meningkatnya kerja dan efektivitas kerja dalam kehidupan manusia sehari-harinya, serta dapat *recover* apa yang ada.. Dampak negatif dari adamya komputer forensik juga ada, dengan adanya itu kejahatan digital juga bertambah dengan akal-akalan manusia supaya tidak masuk ke dalam proses hukum kejahatannya.
3. Contoh kasus kompuetr forensik adalah :

   MEMBONGKAR KORUPSI DAN FRAUD

   Coba copy satu file microsoft word anda dari satu folder ke folder yang lain. Kemudian klik kanan dan bandingkan ‘properties’ di masing-masing file. Kalau kita sekedar ‘copy’ dan ‘paste’, di masing-masing file

itu akan terdapat perbedaan dalam informasi file ‘created’, ‘modified’, dan ‘accessed’ (lihat bagian yang ditandai kotak warna merah). Itu berarti file tidak dianggap ‘otentik’ lagi karena sudah ada perubahan/perbedaan dari kondisi awal.
Di situlah letak keistimewaan IT forensik, dengan hardware atau software khusus, data yang diambil untuk dianalisa akan benar-benar otentik atau persis sama sesuai dengan aslinya. Lebih istimewa lagi, software IT forensik juga dapat memeriksa data atau file bahkan yang sudah terhapus sekalipun (biasanya pelaku korupsi atau fraud berupaya menghilangkan jejak kejahatannya dengan menghapus file-file tertentu). Beberapa vendor yang menyediakan teknologi IT forensik misalnya Paraben, Guidance (EnCase), GetData (Mount Image), dll.

Pengertian Komputer Forensik

Komputer forensik merupakan cabang dari ilmu forensik. Komputer forensik kaitannya dengan laptop, desktop, komputer, dan media penyimpanan digital. Komputer forensik itu seperti mata koin dengan dua mata sisi yaitu scientific dan law, keduanya tidak bisa berdiri sendiri. Output dari forensik secara general itu adalah alat bukti hukum yang sah.

Dampak dari Komputer Forensik

Mendapatkan fakta-fakta objektif dari sebuah insiden atau pelanggaran keamanan teknologi informasi. Komputer forensik sangat perlu dilakukan karena biasanya data di perangkat pelaku dikunci, disembunyikan, atau bahkan dihapus untuk menghilangkan barang bukti atau jejak si pelaku. Dengan adanya digital forensik memudahkan pihak penyidik untuk mendapatkan bukti tersebut.

Contoh kasus komputer forensik

Pada bulan Mei lalu terjadi kebocoran data akun di salah satu marketplace di Indonesia yaitu Tokopedia dengan jumlah 91 juta data akun pengguna dan 7 juta data akun

dagang diretas oleh peretas yang mereka jual di Dark Web. Pihak Tokopedia menyatakan bahwa data yang bocor hanyalah data berupa nama, email, alamat dan data pribadi lainnya. Sedangkan untuk data password, akun pelanggan, dan data keuangan para pengguna atau akun dagang di Tokopedia itu dinyatakan aman.

Komputer forensic merupakan campuran bidang ilmu antara hukum dan komputer yang digunakan untuk membantu proses penegakan keadilan dengan bukti yg ditemukan pada komputer dan media penyimpanan digital.

Dengan adanya komputer forensic, maka proses penegakan keadilan untuk kejahatan digital akan sangat terbantu, karena mudahnya proses penyelidikan berupa pengumpulan barang bukti atau jejak digital yang digunakan untuk investigasi sehingga akan mengarah kepada pelaku. Berikut merupakan contoh kasus yang melibatkan komputer forensic :

Kasus TrioMacan 2000 pada tahun 2014.

Kasus ini merupakan kasus kejahatan digital berupa perbuatan tidak menyenangkan, pemerasan, dan pencucian uang melalui akun twitter. Setelah dilakukan pemeriksaan secara non digital seperti dengan wawancara dan sebagainya, tersangka tidak mengakui bahwa tersangka merupakan admin akun twitter tersebut. Dengan bantuan dari komputer forensic pada pihak Penyidik Cyber Crime Direktorat Kriminal Khusus Polda Metro Jaya sehingga dilakukannya proses pemeriksaan jejak digital berupa rekam ketik di komputer, laptop, dan ponsel millik para tersangka.

Dengan hasil investigasi pada jejak digital tersangka, maka dihasilkan sebuah putusan untuk para tersangka yang ditetapkan bersalah atas tindak pemerasan yang dilakukan berdasarkan Undang-Undang Informasi dan Transaksi Elektronik dan mendapatkan vonis 5 tahun penjara.

Menurut Ruby Alamsyah, komputer forensik atau digital forensik ialah suatu ilmu yang menganalisis barang bukti secara digital hingga dapat dipertanggung jawabkan di pengadilan. Dapat disimpulkan bahwa Komputer Forensik adalah kegiatan mendapatkan bukti digital yang akan digunakan dalam proses hukum. Sebelum diserahkan hukum, bukti-bukti digital harus dianalisis dan verifikasi agar tidak tertipu bahwa buktinya palsu. Kategori barang bukti digital antara lain seperti: laptop, handphone, atau perangkat teknologi yang memiliki tempat penyimpanan dan data dapat dianalisa.

Dampak dari komputer forensik dialami oleh kedua pihak yaitu pihak pelaku kejahatan dan penyidik. Pihak pelaku harus ekstra pada persiapan maupun setelah serangan agar tidak meninggalkan jejak digital seperti tidak meninggalkan alamat ip dan log pada server. Untuk pada penyidik bukti sangat penting untuk mendapatkan pelaku.

Contoh kasus penggunaan forensic komputer adalah pembobolan terhadap tiket[dot]com yang dilakukan oleh empat pelaku SH, MKU, AI, dan MTN. Awalnya, SH melakukan kesalahan yaitu dengan langsung mengumbar

ke sosial media bahwa telah memberi tahu bug pada website tiket[dot]com disaat sebelum melakukan kegiatan yang merugikan. Bila tujuan awalnya untuk memberi tahu untuk kerja sama kepada mereka, sebaiknya mengirim pesan email saja daripada mengumbar ke publik. Selanjutnya, kemungkinan untuk mendapatkan password akun admin adalah melakukan teknik bruteforce dengan table rainbow, ini msh cukup efektif bila pakai hash tanpa key tambahan. Kesalahan fatal selanjutnya meninggalkan kemungkinan meninggalkan jejak seperti masih menggunakan nomor yang sama. Setelah melakukan serangan sebaiknya ganti kartu karena membuat kita menjadi anonim baru.

KOMPUTER FORENSIK

Pengertian Komputer Forensik

Komputer Forensik adalah salah satu teknik penyelidikan atau investigasi beserta dengan analisis menggunakan metode pengumpulan data dan memberikan bukti legal yang didapat pada komputer, penyimpanan data, dan media digital. Komputer forensik tercipta dari penggabungan antarra dua keilmuan, yaitu hukum dan komputer.

Dampak Komputer Forensik

Dampak komputer forensik sangat baragam, dari dampak positif maupun dampak negatif. Dilihat dari dampak positif komputer forensik mampu digunakan dalam mendeteksi atau mencegah dalam kesalahan atas bukti yang disimpan secara digital. Komputer forensik menjadi salah satu bukti konkret atas sebuah kasus penyelidikan. Dilihat dari dampak komputer forensik sendiri tidak lepas dari perkembangan dari ilmu itu sendiri, artinya ilmu komputer forensik sendiri memliki metode yang dibilang masih terbatas.

Contoh Kasus Komputer Forensik

Kasus kopi sianida yang terjadi pada 6 Januari 2016, dimana terdapat korban meninggal dunia atas kasus ini yaitu Mirna Salihin. Mirna Salihin meninggal dunia karena meminum kopi Vietnam di Cafe Olivier, Grand Indonesia.

Pada kasus ini saksi ahli forensik turut hadir untuk memaparkan hasil analisanya terhadap barang bukti yang sudah dikumpulkan oleh penyidik. Barang bukti tersebut berupa USB Flashdisk yang menyimpan video CCTV tempat kejadian perkara. Video CCTV yang diberikan berupa hasil ekstrasi dari DVR sistem monitoring CCTV di Cafe Olivier.

Pada kasus kopi sianida, pendapat para ahli forensik menyebutkan bahwa CCTV yang diberikan oleh penyidik merupakan hasil kloning atau sudah tidak asli sehingga tidak dapat dijadikan barang bukti yang menjerat palaku (Jessica).

Definisi Komputer Forensik

Yaitu ilmu untuk melakukan proses ilmiah dalam mengumpulkan lalu menganalisa data yang diperoleh dari perangkat komputer untuk mendukung penyelidikan atau investigasi. Kolaborasi antara hukum dan komputer sehingga menghasilkan keputusan yang paling tepat untuk diambil oleh pihak pengadilan.

Dampak Komputer Forensik

Komputer forensik memiliki dampak positif yaitu dapat meningkatkan efisiensi juga efektivitas pihak berwajib untuk memperoleh bukti guna memberatkan pihak yang bersalah dan juga menurunkan presentase pengadilan dalam mengambil keputusan yang kurang tepat. Namun komputer forensik juga memiliki dampak negatif yaitu rendah nya hak privasi setiap individu yang melakukan kegiatan menggunakan media komputer karena sewaktu – waktu dapat diperoleh paksa data individu baik positif maupun negatif untuk kepentingan penyelidikan.

Contoh Komputer Forensik

Pada tahun 2009 silam, terjadi sebuah penangkapan yang berlokasi di kota solo sehingga dapat diperoleh sebuah laptop yang diduga dimiliki oleh Noordin M. Top yang berisi video rekaman dua orang sedang melakukan survei target sasaran pemboman pada hotel mewah yang berlokasi di Jakarta yaitu Ritz Carlton dan JW Marriot.

Survei pertama dilakukan pada tanggal 21 Juni 2009 sekitar pukul 07.33, mereka bertiga memantau lokasi peledakan. Mereka berada di lapangan sekitar lokasi kedua hotel tersebut. Pada tanggal 28 Juni 2009 survei kedua dilakukan sekitar pukul 17.40. survei tersebut merupakan kunjungan terakhir sebelum pemboman dilakukan.

Video yang diperoleh oleh polri merupakan contoh implementasi komputer forensik sehingga pelaku pemboman dapat diketahui identitas nya yaitu Dani Dwi Permana dan Nana Ichwan Maulana dan tindakan preventif dapat dilakukan dengan penelusuran kelompok teroris yang terkait oleh kedua pelaku agar tragedi meledaknya bom di tempat umum tidak terjadi kembali.

1. **Apa itu Komputer Forensik**

   Komputer forensik atau yang biasa disebut dengan digital forensik merupakan salah satu cabang ilmu dalam bidang ilmu forensik yang membahas tentang masalah yang berhubungan dengan penyelidikan, identifikasi, pengambilan keputusan dan penyaringan bukti terhadap kejahatan digital menggunakan software dalam pengambil bukti tindak kejahatan kriminal yang dilakukan sehingga informasi yang dihasilkan dapat berbentuk format digital. Tujuan adanya Komputer Forensik adalah untuk dapat memulihkan dan menganalisa sehingga dapat memberikan informasi baik fakta dan opini terhadap suatu permasalahan digital.

2. **Dampak Komputer Forensik**

   Dampak positif dengan adanya komputer forensik diantaranya ;

   1. Setiap pelaku kriminal akan memulai berpikir lagi untuk melakukan tindakan kejahatan digital terhadap suatu individu, ataupun suatu

organisasi karena proses pemberian barang bukti digital dapat dengan mudah diberikan.

2. Membantu dalam menjaga informasi perting terhadap resiko yang mungkin dapat bocor melalui mitigasi resiko

3. Contoh Kasus Komputer Forensik

Forensik Digital forensik bisa dimanfaatkan untuk ruang lingkup yang lebih luas. Tak hanya untuk 'membedah' isi komputer dan ponsel, namun juga untuk melacak lalu lintas rekening bank seperti di kasus Bank Century.

Pakar digital forensik, Ruby Alamsyah menjelaskan, digital forensik adalah menganalisa barang bukti digital secara ilmiah dan bisa dipertanggung jawabkan di depan hukum. Jadi digital forensik ini juga tak harus membahas soal cyber crime (kejahatan di internet). Kasus Century juga bisa diperiksa dengan digital forensik. Pemeriksaan bisa dilacak dari rekaman elektronik transfer dana di bank bermasalah tersebut karena saat ini pembukuan di bank tak lagi manual.

Kemampuan lain dari digital forensik juga bisa 'membedah' kasus Intelectual Property seperti pembajakan cakram digital bajakan serta tindak penculikan dan perampokan dengan memafaatkan rekaman CCTV. Jadi tak hanya komputer yang bisa 'dibedah'. Maka dari itu, istilah digital forensik sempat diubah dari sebelumnya menggunakan sebutan komputer forensik.

1. Definisi Komputer Forensik

   Komputer forensik yaitu cabang dari ilmu forensik, dimana ilmu tersebut sering digunakan sebagai bukti dalam proses hukum untuk mengungkapkan kejahatan atau kriminal secara digital yang didapati di dalam komputer baik itu software maupun hardware.

2. Dampak Komputer Forensik

   Komputer forensik memiliki beberapa dampak yaitu :

- Dapat mengungkapkan suatu kejahatan dengan bukti. Dimana bukti tersebut dapat berupa gambar, teks, audio, maupun video.
- Membantu pihak berwenang seperti polisi dan kejaksaan dalam menangani kejahatan terutama kejahatan yang dilakukan secara digital.
- Dapat memperbaiki data yang telah rusak atau gagal di dalam komputer.

3. Contoh Kasus Komputer Forensik

Pada tahun 2006, terjadi kasus pembunuhan terhadap istri yang dilakukan oleh suaminya sendiri. Suaminya adalah seorang mantan menteri baptis di Texas yang bernama Matt Baker. Matt Baker melakukan pembunuhannya dengan cara memberikan pil tidur dan mencekik leher istrinya. Matt Baker juga melakukan perselingkuhan dengan Vanessa Bulls. Pada kasus pembunuhan ini Vanessa Bulls menjadi saksi, ia menceritakan bahwa Matt Baker memberikan pil tidur dan memborgol kedua

tangan istrinya dan mencekiknya. Tim forensik menyelidiki kasus ini, bahwa Matt Baker mencari pil tidur di beberapa situs web dan juga menggunakan laptop yang diberikan oleh gereja untuk melihat situs-situs yang berkaitan dengan pornografi dan orang-orang yang telah menikah yang ingin melakukan perselingkuhan. Atas kasusnya tersebut Matt Baker dijatuhi hukuman selama 65 tahun.

Apa itu Komputer Forensik?

Komputer forensik secara Bahasa berarti "pencarian fakta pada perangkat elektronik / digital (terutama komputer)". Namun, secara umum, dapat diartikan sebagai "pencarian bukti hukum dalam komputer dan media penyimpanannya".

Tujuan dari disiplin ilmu komputer forensik adalah untuk membantu pemecahan kasus yang menyangkut perangkat digital. Pihak berwajib akan melacak sumber bukti, kemudian mengamankan bukti tersebut, dan akhirnya diproses (dianalisis) demi

kepentingan hukum. Hal ini dilakukan untuk mencari pelaku yang tidak bertanggung jawab.

Tahapan komputer forensik dimulai dengan Pengumpulan Data, yaitu pihak berwajib mengumpulkan sumber-sumber potensial asal data. Kemudian dilakukan Pengujian, yaitu penilaian data-data yang telah dikumpulkan. Lalu dilaksanakan Analisa, yaitu proses untuk menarik kesimpulan. Dan terakhir dibuat Laporan, yaitu penyajian hasil analisa yang didapat.

Dampak dari Komputer Forensik?

Berikut ini adalah dampak atau manfaat Komputer Forensik :

- Membantu proses peradilan.
- Mendapatkan bukti.
- Alat penegak hukum memberantas kriminal.
- Pengumpulan data, bisa untuk pemulihan, analisa, atau representasi.
- Pelacakan secara online / digital.

Contoh kasus Komputer Forensik?

Salah satu contoh penerapan Koputer Forensik adalah kasus Penipuan Online di Banyuwangi (Juni 2020). Sebuah sindikat yang memanfaatkan peretasan nomor HP dan menggunakan aplikasi WhatsApp, melakukan penyamaran dengan niat meminjam uang ke sejumlah korban. Setelah uang didapat, pelaku mencoba melarikan diri. Selain penyamaran, ada juga berbagai modus lainnya.

Polresta Banyuwangi berhasil mengungkap kasus ini setekah laporan adanya nomor HP dan WA yang diretas. Melalui pelacakan digital (menggunakan komputer forensik), Patroli Siber berhasil menemukan nomor dan aplikasi yang diretas itu, ke sejumlah lokasi. Polisi mendapatkan puluhan kartu ATM dan ratusan rekening, HP sebagai alat kejahatan, dan uang bernilai miliaran. 3 pelaku sudah tertangkap, 14 lainnya masih buron

Dari kasus ini, dengan menggunakan komputer forensik, polisi berhasil melacak para pelaku dan keberadaannya. Polisi juga berhasil melacak sejumlah rekening yang digunakan sindikat, menggunakan ilmu

komputer forensik. Hal ini menunjukkan manfaat komputer forensik dalam memberantas tindak kriminal.

Seiring dengan perkembangan jaman yang mulai bersiap menuju Industry 5.0, tidak sedikit yang menyalahgunakan kemudahan teknologi yang berkembang ke arah yang salah. Maraknya tindak kriminal yang mulai merugikan kelompok masyarakat membuat pemerintahan khususnya di Indonesia mulai mengeluarkan Undang Undang yang mengatur tentang informasi serta transaksi elektronik, atau teknologi informasi secara umum, yang dinamakan dengan UU ITE.

Dalam penegakan hukum dibidang ITE inilah dibutuhkan suatu teknik atau ilmu untuk menemukan, menganalisis dan menginvestigasi bukti bukti yang sah secara hukum mengenai tindak kriminal yang menggunakan media digital. Ilmu ini disebut dengan Komputer Forensik.

Dampak dengan adanya Komputer Forensik, para pengguna teknologi akan lebih bijak dan berhati hati dalam penggunaan teknologi digital. Serta dapat membantu mencari bukti bukti pendukung yang dibutuhkan jika sewaktu waktu terjadi tindak kriminal

pada suatu organisasi atau perusahaan. Perlu diketahui, ilmu ini dapat digunakan dalam berbagai situasi seperti ketika terjadinya kebocoran informasi suatu perusahaan baik secara disengaja maupun tidak disengaja, kejahatan yang berkaitan dengan finansial, serta kasus penipuan, pencurian serta pelecehan seksual.

Contoh kasus yang melibatkan ilmu Komputer Forensic sebagai pendukung bukti bukti tindak kejahatan yaitu, pada kasus yang tidak lama terjadi pada Kamis 08 Oktober 2020 ketika aksi demonstrasi penolakan *Omnibus Law*. Pada hari itu, sejumlah oknum melakukan aksi perusakan fasilitas umum khususnya pada pembakaran Halte Sarinah, Jakarta. Kemudian dalam pencarian pelaku dilakukan investigasi melalui media digital seperti CCTV dan media sosial. Para investigasi menggunakan metode Open Source Intelligent dalam pencarian pelaku, sehingga dengan dukungan ilmu dan metode ini lah pihak hukum dapat mengungkapkan pelaku pembakaran halte di Jakarta.

Contoh kasus lainnya yang melibatkan ilmu komputer forensic yaitu pada kasus hilangnya uang tabungan Winda

Earl di Maybank Indonesia. Dimana lebih dari Rp 20 miliar hilang dari tabungan korban. Sampai saat ini kasus ini masih dalam proses penanganan hukum. Penginvestigasian masih dilakukan untuk pencarian bukti bukti pendukung pada setiap media terkait seperti pada perangkat penyimpanan, termasuk penyeledikan pada system keamanan Maybank Indonesia. Tentu saja pengumpulan bukti digital harus dilakukan melalui prosedur sehingga nilai pembuktian dari bukti digital dapat diterima dalam proses hukum. Tersangka yang ditetapkan saat ini merupakan Kepala Cabang Maybank Indonesia Cipulir Jakarta Selatan berinisial A.

1. Apa itu Komputer Forensik?

   Jawab : Komputer Forensi merupakan suatu Teknik yang dilakukan untuk proses penyelidikan dan analisis komputer untuk mengumpulkan berbagai bukti berupa data dengan persoalan hukum yang tengah diselidiki.

2. Apa dampak dari komputer forensic?

   Jawab : computer forensic memberikan banyak sekali dampak di berbagai kasus, seperti diperolehnya informasi pada proses penyelidikan perkara baik pidana maupun perdata, pada bidang kedokteran diperolehnya informasi dalam melakuakn penelitian atau visum, dan pada bidang hukum dapat digunakan dalam proses pencarian alat bukti dan materi dalam persidangan.

3. Sebutkan contoh kasus komputer forensic!

   Jawab :

   Salah satu contoh kasus komputer forensic adalah dianalisnya rekaman CCTV di kafe Olivier pada kasus pembunuhan Mirna. Hasil dari analisis rekaman tersebut adalah titik rawan sianida yang ditaruh dalam es kopi Vietnam yang diminum oleh Mirna selama 4 menit, menurut ahli digital forensik Polri, AKBP Muhammad Nuh. Empat menut yang dimaksud oleh Nuh adalah mulai dari pukul 16.29 hingga 16.33. pada pukul 16.29, Terdakwa Jessica diketahui melakukan gerakan

membuka tas yang terekam dengan jelas dalam CCTV.

Didasari dari 2 suku kata yaitu komputer dan forensik. Komputer adalah perngakat elektronik yang mampu memanipulasi informasi dan data. Forensik adalah sebuah suatu proses ilmiah yang didasari oleh ilmu pengetahuan dalam mengumpulkan, menganalisa dan menghadirkan berbagai bukti dalam sidang pengadilan dikarenakan suatu kasus hukum. Jadi komputer forensik adalah pengumpulan dan analisa data dari berbagai sumber daya komputer yang layak untuk disajikan dalam pengadilan dikarenakan suatu kasus hukum.

Dampak dari komputer forensik

Dampak dari komputer forensik dianataranya

- Organisasi atau perusahaan dapat selalu siap dan tanggap seandainya ada tuntutan hukum yang melanda dirinya, terutama dalam mempersiapkan bukti-bukti pendukung yang dibutuhkan;
- dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir;

- Para kriminal atau pelaku kejahatan akan berpikir dua kali sebelum menjalankan aksi kejahatannya terhadap organisasi atau perusahaan tertentu yang memiliki kapabilitas forensik komputer
- Membantu organisasi atau perusahaan dalam melakukan mitigasi resiko teknologi informasi yang dimilikinya.

Contoh kasus komputer forensik

Salah satu contoh kejahatan yang menggunakan teknologi informasi adalah kasus obrolan mesra yang menjerat Habib Rizieq dan Firza Husain di salah satu media sosial pada awal tahun 2017 silam. Kegunaan komputer forensik adalah mendapatkan informasi dan data untuk dijadikan bukti. Barang bukti yang diterima oleh pengadilan harus bersifat otentik, lengkap, handal dan terpercaya.Tanpa mekanisme perlindungan data, data tersebut dapat dengan mudah dimanipulasi. Dengan demikian, pengadilan sekarang harus menuntut persyaratan yang ketat pada diterimanya bukti digital di

pengadilan. Oleh karena itu dibutuhkan ahli dalam bidang komputer forensik

APA ITU KOMPUTER FORENSIK :

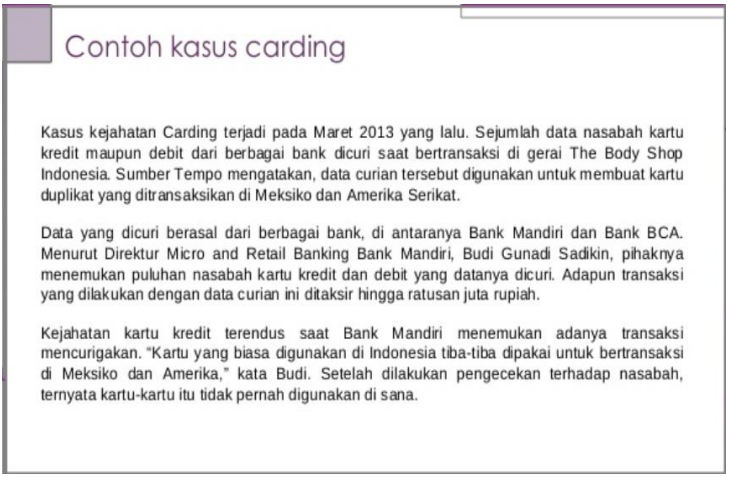
Komputer forensik adalah suatu ilmu yang mempelajari tentang kejahatan digital, dengan menggabungkan antara ilmu hukum dan komputer sehingga dapat menemukan kejahatan yang diterjadi di dalam digital. komputer forensik ini juga adalah salah satu cabang ilmu dari forensik.

Menurut Ruby Alamsyah sebagai ahli, “komputer forensik atau digital forensik ialah suatu ilmu yang menganalisis barang bukti secara digital hingga dapat dipertanggungjawabkan di pengadilan. Yang termasuk barang bukti digital tersebut antara lain: laptop, handphone, notebook, dan alat teknologi lain yang memiliki tempat penyimpanan dan dapat dianalisa.“

DAMPAK DARI KOMPUTER FORENSIK :

- Dapat mempermudah manusia ataupun penyelidik dalam mencari bukti digital dalam sebuah kasus ataupun kajahatan digital
- Dapat mempermudah untuk memulihkan data di dalam komputer ataupun software dan hardware lainnya yang terkena hack

CONTOH KASUS KOMPUTER FORENSIK :



Menurut Dr. HB Wolfre, Komputer Forensik adalah Serangkaian metodologi teknik dan prosedur pengumpulan bukti, dari peralatan komputasi dan

berbagai perangkat penyimpanan dan media digital, yang dapat disajikan di pengadilan dalam format yang koheren dan bermakna.

Dengan begitu tujuan utama dari aktivitas forensik komputer adalah sebagai berikut:

1. Membantu memulihkan, menganalisa dan mempresentasikan materi berbasis digital/elektronik sehingga dapat digunakan sebagai alat bukti yang sah di pengadilan
2. Mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivitasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud.

Dengan adanya komputer forensik, memiliki berbagai macam manfaat, diantaranya:

- Persiapan bukti hukum seandainya ada tuntutan bagi suatu perusahaan/organisasi
- Seandainya terjadi peristiwa kejahatan yang membutuhkan investigasi lebih lanjut, dampak gangguan terhadap operasional organisasi atau perusahaan dapat diminimalisir

Namun, terlepas dari manfaatnya, dengan adanya komputer forensik juga menimbulkan hal-hal negatif, yaitu:

- Karena ilmu baru, sehingga SDM yang memiliki keahlian khusus masih terbatas
- Dengan berkembangnya teknologi yang cepat, semakin pintar dan terampil pula para pelaku kejahatan teknologi informasi dan komunikasi yang ditandai dengan makin beragamnya dan kompleksnya jenis-jenis serangan serta kejahatan teknologi yang berkembang.

CONTOH KASUS

Kasus Winda Lunardi yang kehilangan uang sebesar Rp 22 Miliar di rekening tabungannya. (Maybank)

Potongan berita : Kasus ini bermula saat atlet e-sport Winda "Earl" Lunardi melaporkan ke Badan Reserse Kriminal (Bareskrim) Polri perihal uang tabungan miliknya dan sang ibunda, Floleta, senilai Rp 20 miliar yang raib. Besaran dana kemudian disebutkan oleh Kuasa Hukum Maybank yakni Hotman Paris yakni Rp 22 miliar.

Forensik adalah proses menggunakan ilmu pengetahuan untuk mengumpulkan, menganalisis dan menyajikan bukti di pengadilan. Forensik biasanya berhubungan dengan pemulihan dan analisis barang bukti. Barang bukti dapat berupa sidik jari atau dna. Namun karena komputer forensik adalah disiplin ilmu yang baru, sehingga masih sedikit standarisasi dan konsistensi di setiap pengadilan. Akibatnya belum diakui sebagai disiplin ilmu ilmiah. Sehingga bisa didsefinisikan bahwa komputer forensik adalah *disiplin ilmu yang menggabungkan elemen dari hukum dan ilmu komputer untuk mengumpulkan dan menganalisis data dari sistem komputer, jaringan, komunikasi nirkabel dan media penyimpanan dengan cara yang bisa diterima sebagai bukti di pengadilan*.

Komputer forensik memiliki dampak yang sangat luas, salah satunya adalah digunakan untuk mengungkap banyak kasus kriminal seperti pembunuhan, penculikan, pencurian dll. Dengan adanya komputer forensik, bukti bisa ditelusuri dari data yang tersimpan di dalam sistem. Karena tujuan utama dari komputer forensik sendiri ialah untuk identifikasi, mengumpulkan, menyajikan, dan menganalisis data dengan menjaga integritas dari setiap bukti yang dikumpulkan sehingga bisa digunakan dalam pengadilan sebgai barang bukti yang sah

Contoh kasus komputer forensik adalah kasus yang bulan lalu ini hangat dibicarakan di media sosial yaitu kasus pembakaran beberapa halte di Jakarta dalam unjuk rasa penolakan Undang-undang Cipta Kerja. Dalam video yang disajikan Mata Najwa, penelusuran dilakukan untuk membuktikan siapa pelaku dari pembakaran beberapa halte ini. Banyak tuduhan yang ditujukan kepada demonstran bahwa para demonstranlah pelaku pembakaran. Dengan menganalisis dari setiap video yang telah direkam oleh para demonstran yang turun langsung ke tempat kejadian dan juga memakai rekaman CCTV

dari lokasi kejadian yang bisa diakses publik, bahwa dari ciri-ciri pelaku seperti memakai pakaian serba hitam yang mana pelaku berada di dekat tempat kejadian perkara. Pelaku juga bertindak aneh di tempat kejadian perkara dan peneluran lebih lanjut diserahkan ke Mabes Polri agar kasus bisa terungkap.

Komputer forensik atau disebut juga digital forensik merupakan cabang dari ilmu forensik yang menerapkan teknik investigasi dan analisis untuk mengumpulkan dan mengamankan bukti-bukti dari perangkat komputer (digital) untuk keperluan hukum. Komputer forensik merupakan alat yang penting dan dibutuhkan dalam hal untuk melawan kejahatan siber (cybercrime). Tujuan dari komputer forensik ini adalah untuk melakukan penyelidikan secara pada perangkat komputer sehingga mendapatkan bukti-bukti agar dapat diketahui apa yang sebenarnya terjadi dan siapa yang bertanggung jawab atas kejadian tersebut. Dan juga mengumpulkan bukti-bukti tersebut dalam bentuk laporan untuk dibawa ke pengadilan dan diproses secara hukum.

Dengan perkembangan teknologi yang semakin canggih, hal itu berdampak pada penggunaan bidang komputer forensik yang semakin luas dan beragam. Komputer forensik dapat digunakan untuk membantu proses penegakkan hukum seperti untuk melakukan investigasi terhadap penipuan, transaksi gelap, tindakan kriminal, kekerasan, cyber bullying, pencurian data atau properti seseorang/organisasi, peretasan, serta penggunaan internet yang tidak pantas,

Contoh kasus dari komputer/digital forensik ini dapat dilihat pada kasus "kopi sianida" yang ramai menjadi perbincangan pada tahun 2016 lalu. Jessica Kumala Wongso, yang diduga meracuni sahabatnya sendiri, Wayan Mirna Salihin, dengan racun sianida yang dicampurkan ke es kopi Vietnam pesanannya di Kafe Olivier pada 6 Januari 2016 silam yang menyebabkan Jessica divonis 20 tahun penjara. Pada salah satu persidangan saat itu, JPU mendatangi ahli digital forensik untuk menjelaskan bukti berupa flashdisk USB yang berisi rekaman CCTV dari DVR di Kafe Olivier. Pada sidang selanjutnya, pihak terdakwa (Jessica) mendatangi

Ahli IT yang menyebut kalau rekaman CCTV yang digunakan sebagai bukti sudah melewati proses editing yang bertujuan untuk memojokkan terdakwa. Setelah persidangan, muncul artikel-artikel di internet yang menyebut bahwa "Jessica dijerat CCTV hasil cloning" yang dianggap sebagai rekaman CCTV hasil editan/manipulasi. Namun pada faktanya, Josua Sinambela, seorang ahli digital forensik, menyatakan bahwa tindakan mengedit rekaman barang bukti itu sah-sah saja asal mengikuti prosedur yang berlaku. Disini dapat dilihat implementasi dari proses digital forensik. Josua mengatakan bahwa penyidik akan meminta bantuan kepada ahli digital forensik untuk melakukan analisis terhadap rekaman yang akan dijadikan barang bukti. Tahapan awal dari digital forensik adalah melakukan imaging/bit stream copy, yaitu melakukan duplikasi barang bukti asli (master) ke media penyimpanan lain (HDD, USB, DVD, dll) dalam bentuk salinan yang identik yang harus memiliki nilai hash/check integritas yang sama untuk dianalisa oleh ahli digital forensik. Orang awam menyebut proses imaging/bit stream copy dengan istilah cloning. Josua mengatakan juga untuk

mempermudah menganalisis video, ahli digital forensik sah-sah saja melakukan composting (menggabungkan) video dan melakukan enhancement video (zooming, meningkatkan kualitas gambar/contrast dengan algoritma tertentu) tapi tanpa mengubah informasi atau kejadian sesungguhnya dan harus sama dengan rekaman yang ada pada file master.

Pengantar Forensik Teknologi Inf.

1. Apa itu komputer forensik

   >> Komputer forensik adalah cabang ilmu yang mempelajari teknik untuk melakukan penyelidikan dan analisis untuk mengumpulkan dan memberikan bukti-bukti data yang berada di sebuah komputer yang ada hubungannya dengan persoalan hukum yang sedang diselidiki dan bertujuan untuk melakukan penyelidikan terstuktur dan sistematis di dalam pencarian bukti-bukti data.

2. Dampak komputer forensik

   >> Terdapat dampak positif dan negatif terhadap adanya komputer forensik, untuk dampak positif yaitu dapat menyelesaikan kasus-kasus cybercrime di dalam dunia maya. Dan untuk dampak negatifnya adalah penggunaan teknik deepfake yaitu rekayasa gambar maupun suara sehingga pelaku kejahatan dapat membuat hal-hal yang tidak diinginkan.

3. Contoh kasus komputer forensik

   >> Beberapa tahun yang lalu, Indonesia dikejutkan oleh kasus pembunuhan seorang artis, Alda, yang dibunuh di sebuah hotel di Jakarta Timur. Ruby Alamsyah selaku ahli forensik menganalisa video CCTV yang terekam di dalam harddisk di sebuah server. Ruby memeriksanya untuk mengetahui siapa saja yang datang dan keluar hotel tersebut. Namun, saat itu awareness terhadap digital forensik dapat dikatakan kurang bahkan belum ada sama sekali. Sehingga, pada hari kedua setelah pembunuhan, Ruby ditelepon untuk

diminta bantuan untuk menangani digital forensik. Sangat disayangkan bahwa kepolisian tidak mempersiapkan barang bukti yang asli dengan baik. Seharusnya barang bukti tersebut dikarantina sejak awal dan dapat diserahkan kepada Ruby bisa kapan saja asalkan sudah dikarantina. Dua minggu setelah peristiwa alat tersebut diserahkan kepada Ruby, tapi saat ia periksa alat tersebut ternyata sejak hari kedua kejadian sampai ia terima masih berjalan merekam. Akhirnya tertimpalah data yang penting karena CCTV di masing-masing tempat/hotel berbeda settingnya. Akibat hal tersebut, barang bukti pertama tertimpa sehingga tidak berhasil diambil datanya.

Komputer Forensik merupakan suatu aktivitas untuk melakukan kegiatan penyelidikan beserta analisis yang bertujuan untuk mengumpulkan bukti – bukti sebagai alat untuk mengungkap sebuah kasus yang dapat dipertanggungjawabkan secara hukum.

Komputer forensik mempunyai dampak positif dan dampak negatif. Untuk dampak positifnya komputer forensik dapat membantu membantu menyelesaikan kasus tindak pidana korupsi contohnya dengan melakukan penyadapan suara. Untuk dampak negatifnya komputer forensik seperti yang terjadi pada akhir akhir ini yaitu menggunakan deepfake yaitu teknik video rekayasa yang dibuat oleh kecerdasan buatan sehingga menghasilkan gambar dan suara yang terlihat dan terdengar asli.

Contoh kasus Komputer Forensik

Dikutip dari Liputan6.com Jakarta - Pada akhir Juli lalu, para pengguna Ashley Madison dibuat was-was setelah situs pencarian pasangan selingkuh itu mengalami serangan cyber. Kelompok hacker yang mengidentifikasikan dirinya sebagai “The Impact Team”

mengklaim telah berhasil menguasai data pribadi 37 juta pengguna Ashley Madison. Menurut laporan terbaru, ulah usil hacker tersebut tidak saja merugikan Ashley Madison, melainkan juga Amazon dan GoDaddy. Dilaporkan laman The Register, Selasa (8/9/2015), sejumlah pengguna Ashley Madison menuntut Amazon Web Services dan GoDaddy selaku penyedia jasa internet (ISP) karena keduanya dianggap memfasilitasi penyebaran bocoran data pribadi yang berhasil dicuri hacker. Kasus yang sangat merugikan Amazon Web Services dan GoDaddy itu kini ditangani oleh Pengadilan Arizona, Amerika Serikat. Para penuntut disebutkan meminta ganti rugi sebesar US $3 juta. Para pengguna situs tersebut juga disebutkan akan segara menyeret Avid Life Media selaku induk usaha Ashleymadison.com ke pengadilan.

Komputer Forensik adalah salah satu cabang dari ilmu forensic, forensic adalah ilmu pengetahuan yang digunakan untuk membantu proses sebuah penegakan keadilan dengan cara ilmiah. Jadi Komputer Forensik bisa dibilang sebuah cara atau proses yang membeantu sebuah

penegeakan keadilan dengan menerapkan teknik investigasi dan analisi dalam mengumpulkan dan menyimpan bukti dari perangkat Komputasi.

Dampak adanya Komputer Forensik adalah menegakan keadilan di dalam dunia cyber, jadi jika ada sebuah masalah Cyber Crime seperti HOAX, Penghinaan, dsb, maka Komputer forensic yang akan membantu masalah tersebut.

Dikutip dari TribunTernate.com - "Adapun terkait konten-konten tindak pidana hate speech dikelompokkan ke dalam beberapa topik, ada hate speech terhadap presiden," kata Yusri dalam konferensi pers yang disiarkan langsung melalui Instagram Polda Metro Jaya, Senin (4/5/2020). Yusri menjelaskan, tersangka hate speech pertama berinisial NA. Dia ditangkap karena menyebarkan ujaran kebencian terhadap Presiden Jokowi melalui akun Facebook. "Dia menuliskan keterangan, 'Daripada dokter-dokter, lebih baik presiden saja meninggal karena presiden lebih mudah dapat gantinya, apalagi saat ini manfaatnya kecil sekali'," ujar Yusri. Tersangka selanjutnya adalah YH yang ditangkap di

daerah Sukabumi, Jawa Barat dan AFR. Mereka ditangkap karena menyebarkan ujaran kebencian terhadap Presiden Jokowi dan Menteri Kesehatan Terawan Agus Putranto melalui pesan singkat WhatsApp. Kedua tersangka bahkan melampirkan dan menyebarkan foto Menkes Terawan disertai keterangan berisi ujaran kebencian yang meresahkan masyarakat. "Mereka menulis penghinaan dan atau pencemaran nama baik yang menyerang pribadi Presiden RI dan Menkes RI," ujar Yusri. Sementara itu, tujuh orang lainnya ditetapkan sebagai tersangka penyebaran berita hoaks terkait Covid-19 di antaranya berita hoaks terkait penutupan seluruh kantor BUMD DKI akibat Covid-19 dan penutupan akses pintu tol masuk wilayah Jakarta dengan menyertakan logo Polda Metro Jaya.

Para tersangka dijerat Pasal 28 Juncto Pasal 45 Undang-Undang Informasi dan Transaksi Elektronik (ITE) Juncto Pasal 14 UU Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana dan Pasal 207, 208 Ayat 1 KUHP. Ancaman hukumannya adalah 6 hingga 10 tahun kurungan penjara.

Apa itu komputer forensik

Menurut saya pribadi, Komputer forensik itu merupakan suatu analisa terhadap kasus yang berbentuk digital dan dapat dipreses dengan hukum.

Dampak dari Komputer forensik

Dampaknya ialah dapat mengetahui jejak pelaku dari data digital berdasarkan tahapan pengumpulan data, pengujian data, dan analisa data.

Contoh kasus

Contoh kasusnya berasal dari Surabaya. Bermula dari hobi melakukan testing security pada website untuk berharap imbalan secara acak. Namun tidak disangka ia malah mendapatkan web yang berhubungan dengan FBI. Tersangka tersebut masih berstatus mahasiswa yang terdiri dari Katon Primadi Sasmitha (yang merupakan teman satu komunitas dengan saya), Nizar Ananta yang berasal dari Surabaya , Triwardhana Panggau yang berasal dari Banyuwangi.

Ketiga mahasiswa ini masih semester enam di Stikom Surabaya dengan jurusan Sistem Informasi. Mereka ini diduga telah melakukan peretasan lebih dari 600 website di 44 negara menggunakan Teknik SQL Injection. Katon primadi yang saya kenal dia juga merupakan juara 1 untuk kompetisi hacking di Cyber Jawara yang diselenggarakan oleh TNI. Ia memang hobi mencari celah pada website dan sering berbagi tutorialnya di facebook.

Pihak kampus juga masih menelusuri penyebab penangkapan tersebut. Pihak kampus juga masih belum mendapat keterangan dari pihak FBI maupun Polri.

Pihak kampus menjelaskan bahwa tersangka ini merupakan tergolong anak yang pintar yang dilihat dari IPKnya dengan rata-rata 3.00.

Dosen mata kuliah jaringan Komputer Anjik Sukma Aji berkomentar soal ini bahwa peretasan ini dilakukan karena keingintahuan mereka untuk meretas web yang sekian banyaknya dan membutuhkan waktu yang lama dan ada tahapannya. Ia juga menjelaskan bahwa hacker

tujuannya banyak ada yang ingin tahu, mencoba kemampuannya atau hanya sekedar melihat saja.

Pihak kampus juga menghimbau mahasiswanya untuk membaca lagi surat pernyataan mengenai aturan yang ada. Pihak kampus juga sudah memberi pembekalan budi pekerti, softskill, dan hard skill secara regular.

Sugiharto juga berkomentar bahwa ketiga mahasiswanya tersebut sangat aktif di dunia perkuliahan bahkan tidak pernah melakukan penlanggaran. Kesimpulan dari kasus ini ialah untuk berhati-hati hati juga ingin melakukan sesuatu yang tidak memiki tujuan baik.

Pengantar Forensik Teknologi Informatika

Komputer forensik merupakan bidang ilmu yang menggabung antara ilmu hukum dan komputer. Dalam komputer forensik, ilmu komputer digunakan untuk membantu penyidikan dalam suatu kasus hukum. Aktivitas yang dilakukan antara lain identifikasi, pengambilan ataupun penyaringan dokumen bukti komputer yang berhubungan dengan kasus hukum tersebut.

Dampak komputer forensik:

1. Komputer forensic dapat membantu pemulihan dokumen ataupun informasi yang terdaftar melalui komputer ataupun informasi digital yang dapat membantu jalannya proses hukum sipil maupun kejahatan komputer.
2. Komputer forensik dapat menganalisa bukti digital yang didapatkan untuk mendapatkan fakta dari bukti-bukti digital yang didapatkan.

Contoh Kasus:

"Pada tanggal 29 September 2009, Polri akhirnya membedah isi laptop Noordin M. Top yang ditemukan dalam penggrebekan di Solo. Dalam temuan tersebut akhirnya terungkap video rekaman kedua 'pengantin' dalam ledakan bom di Mega Kuningan, Dani Dwi Permana dan Nana Ichwan Maulana.
Sekitar tiga minggu sebelum peledakan Dani Dwi Permana dan Nana Ichwan pada video tersebut setidaknya melakukan field tracking sebanyak dua kali ke lokasi JW. Marriot dan Ritz Carlton yang terletak di

Komputer forensik adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti hukum yang disimpan dalam media penyimpanan digital. Komputer forensik ini biasanya dimanfaatkan dalam beberapa aspek kehidupan. Misalnya digunakan pada suatu kasus penyelidikan tindak kriminal seperti penyebaran hoax, pencemaran nama baik, hate speech dan kasus-kasus lain yang membutuhkan bukti-bukti untuk kepentingan keadilan hukum.

Dampak positif dari komputer forensik antara lain dapat membantu proses hukum untuk menemukan bukti-bukti yang lebih akurat dari suatu tindakan atau kejadian. Bukti yang terekam secara digital akan mempermudah untuk menegakkan keadilan hukum.

Berdasarkan contoh kasus yang menimpa seorang musisi Indonesia bernama Ahmad Dhani, diduga melakukan pencemaran nama baik, di mana Ahamd Dhani membuat konten video yang berisi kata "*idiot*" yang dianggap melecehkan nama baik peserta demo di luar hotel tempat terdakwa menginap.

Apabila melihat dari kasus tersebut, Ahmad Dhani dapat dipidana jika memenuhi unsur yang ada dalam Pasal 27 ayat (3) UU ITE, di mana pengertian dari pencemaran nama baik merujuk pada pasal-pasal mengenai penghinaan yang diatur dalam KUHP. Kasus ini bermula ketika Ahmad Dhani hendak menghadiri acara deklarasi 2019 Ganti Presiden di Surabaya pada 26 Agustus 2018. Acara deklarasi 2019 Ganti Presiden di Tugu Pahlawan itu gagal diselenggarakan, karena didemo oleh sejumlah warga. Ahmad Dhani tidak bisa keluar dari hotel karena dihadang para pengunjuk rasa yang menolak acara deklarasi tersebut.

Karena terjebak di dalam hotel, membuat Ahmad Dhani membuat vlog yang berisi permintaan maaf kepada massa aksi 2019 Ganti Presiden karena tidak bisa keluar hotel. Dia mengatakan dirinya dihadang oleh pendemo pro pemerintah dan mengucapkan kata idiot dalam videonya. Atas pernyataannya, kelompok yang menamakan Koalisi Bela NKRI melaporkan Ahmad Dhani ke Polda Jawa Timur pada 30 Agustus 2018. Kelompok itu merasa Dhani melakukan pencemaran nama baik.

Dapat disimpulkan Ahmad Dhani terjerat Pasal 27 ayat 3 juncto Pasal 45 ayat 3 UU ITE yang merujuk pada Pasal 311 KUHP.

Komputer forensik adalah bagian dari ilmu forensik dimana ilmu ini menggunakan metode atau prosedur untuk memeriksa media komputer, penyimpanan, atau media digital lainnya dengan maksud menemukan bukti atau jejak yang akan memberikan informasi serta fakta yang dapat digunakan pada kasus yang ada. Dampak positif yang ditimbulkan misalnya dengan menyelidiki jejak digital yang ada, didapat sebuah bukti yang membantu dalam sebuah proses pengadilan.

Contoh Kasus : 62 Menit Operasi Pembakaran Halte Sarinah (Laporan disusun oleh Tim Buka Mata Narasi)

Kasus pembakaran halte sarinah ini terjadi pada tanggal 8 Oktober 2020, dimana pembakaran ini terjadi saat berlangsungnya demontrasi menolak Undang – Undang Cipta Kerja. Tim Buka Mata Narasi bermaksud mengungkap apakah benar para demonstran yang membakar halte tersebut atau ada oknum yang memang

datang bertujuan untuk membakar dan memperburuk situasi saat berlangsungnya demonstrasi.

Tim Buka Mata Narasi mengumpulkan data visual dari berbagai sumber seperti foto dan video dari berbagai media sosial termasuk Youtube, Twitter, Instagram dan TikTok serta rekaman CCTV dari lokasi kejadian yang dapat diakses publik. Dengan menggunakan data yang dikumpulkan tersebut Tim Buka Mata Narasi melakukan analisis dan merangkai ulang kejadian yang terjadi pada saat itu. Hasilnya didapat beberapa pelaku yang bekerja sama membakar halte. Dengan menggunakan machine learning berbasis tensorflow, gambar visual dapat diperjelas sehingga wajah pelaku dapat dikenali. Hasil temuan Tim Buka Mata Narasi ini dikonfirmasi ke Polda Metro Jaya dan nantinya akan dikembangkan lebih lanjut oleh tim dari Polda Metro Jaya.

1. **Apa itu Komputer Forensik**

Menurut saya pribadi, Komputer forensik merupakan sebuah cabang ilmu forensik yang berkaitan erat dengan

bukti legal yg ditemui pd computer dan media penyimpanan digital

2. **Dampak dari Komputer Forensik**

Dampak dari komputer forensik adalah susah untuk menghilangkan jejak digital yang sudah tersebar luas di internet. Tetapi disamping itu pelacakan dari jejak pelaku juga dapat diketahui berdasarkan tahapan pengumpulan data, pengujian data, dan analisa data.

3. **Contoh Kasus**

Beberapa tahun lalu ada berita penangkapan seorang carder di Jakarta Barat, dan pada kasus ini ada lagi buronan carder belia bernama **Dicky Pernanda** AKA **Dicky SreetRidder Haw**. Dicky berbelanja di situs **Zalora** dan **Lazada** dengan kartu kredit danamon milik **FW**, dan saat ini berita ini dibuat sedang dilakukan pencarian jika dilihat dari bukti transaksi mungkin bisa jadi berstatus tersangka karena bukti-bukti yang ada sudah kuat jika ingin melaporkan ke kantor polisi.

Diberitahukan dari korban berinisial **FW** di Facebook yang mengungkapkan bahwa kartu kredit nya telah di sebar luaskan oleh orang lain disalah satu grup carding yang bernama **Pencari Receh**, dan disebarkan oleh **Cupuculunz Ganisangrespec**.

Untuk alamat detail tersangka sudah diketahui oleh korban dengan menghubungi pihak Lazada tersebut, berikut adalah screenshotnya:


Berdasarkan pengecekan di sistem kami , kami temukan percobaan transaksi menggunakan kartu kredit dengan 4 digit terakhir [redacted] dengan detail berikut ini :

Merchant Ref No/ No.order : 208113538
Name : DICKY PERNANDA
Address : Jln Jendral sudriman,serandu rt01 rw5 ,depantower Pemalang, Jawa Tengah 52363 id
Phone Number : 085200298606
Email Address : fernanda_dicky@gmail.com
Date/Time: Aug 05 2015 11:08:16 PM
IP Address: 36.72.249.53 | ARIN | RIPE | Medan, SUMATERA UTARA ID
Ammount : 278.000
Status : Invalid

Korban Berinisial FW Mengetahui perihal tentang kartu kreditnya di pakai oleh orang lain bermula ketika FW menerima sms dari lazada yang menginformasikan pembelian menggunakan kartu kredit miliknya pada Jam 10.17 PM waktu setempat, dengan total pembelian barang sebesar **Rp.102.800,00**

Menurut dari keterangan FW *"Sms Notifikasi memang dari Lazada, Tapi setelah subuh , saya menghubungi ke card center dan ternyata ada 4 Transaksi, 2 transaksi yang dilakukan di merchant Lazada dan sukses order, 2 ke merchant Zalora yang satu sukses paid Rp.278.000, tetapi satu lagi gagal merchant. Tersangka melakukan transaksi antara pukul 22.03 sampai pukul 22.10 waktu setempat pada tanggal 5*

Agustus 2015. Kalau dari pihak Lazada saya masih menunggu konfirmasi ".

Korban menjebak Dicky setelah adanya verifikasi data dari pihak zalora dengan menanyakan tentang keaslian data korban, berikut sms verifikasi yang dilakukan FW untuk mengecek keaslian data yang didapatkan :

Untuk data tempat Dicky bersekolah sudah di kantongi oleh FW dan sangat mengejutkan ternyata Dicky ini masih SMP, berikut detail tempat dicky bersekolah:

Identitas		Kontak	
Nama	: SMP NEGERI 4 COMAL	Telepon	: 0285
NPSN	: 20340627	Faximile	: 0285-
Alamat	: Jalan Raya Tumbal Rt 1/ Rw 3	E-mail	: smpneg
Kode Pos	: 52363	Website	:
Desa/Kelurahan	: TUMBAL		
Kecamatan/Kota (LN)	: Kec. Comal		
Kab.-Kota/Negara (LN)	: Kab. Pemalang		
Propinsi/Luar Negeri (LN)	: Prop. Jawa Tengah		
Status Sekolah	: NEGERI		
Waktu Penyelenggaraan	: Pagi		
Jenjang Pendidikan	: SMP		

Setelah beberapa hari berita ini tersebar si Dicky memakai kartu kredit FW, berikut wall terakhir Dicky di Facebook sebelum dihapus olehnya:

Setelah dicoba di hubungi Dicky tampak merasa tertekan dan akhirnya menutup akun fb nya serta menghapus wall di facebook, ini bukti bahwa si dicky ketakukan dan sudah tertekan secara batin hingga keluar status di wall FB nya si dicky seperti berikut


XL 3G
3:41 PM
93%
Dicky SreetRidder Haw
In about 3 months
About
Photos
Friends
Dicky SreetRidder Haw
55 mins
yAllah :'(semoga cpt kelar :'(sumpah w gtw apa" .. Kok bsa jd gni :'(kapok dan sngt menyesal :'(
Berawal dr iseng dan coba" :'(semoga bpknya mau maafin saya :'(..
6 Likes
Like
Comment
Share


14:15
Dicky SreetRidder Haw
Hai Dicky , Jawab dong...
apa pak
pak ?
Pak Sumpah saya g tau apa"
saya dpt cc nya pak f .. dari org sbare
ane cuman bantu klll
pak .. tolong pak
Sumpah saya g tau apa" ...
uang udh dl refund,saya ngaku salah
Tolong Pak ,, Sampaikan pada pak f saya minta maaf dan saya mengaku salah
saya sangat menyesal ..
*pak .. tolong pak .. prtlmbangkan sya mh mau sekolah
Jangan gt pak TOLONG pak .. mhonn ...

Mungkin si dicky sudah benar-benar kapok. Menurut saya yang harus bertanggung jawab dalam hal ini adalah penyebar kartu kredit tersebut serta orang tua si Dicky karena mengingat umur Dicky yang masih SMP, Dicky masih menjadi tanggung jawab orang tuanya.

CYBERCRIME

Pernah mendengar istilah cyber crime, sudah tahu pengertian cyber crime itu apa?

Istilah tersebut belakangan kerap terdengar seiring dengan perkembangan dunia digital.

Cyber crime atau kejahatan di dunia maya sendiri merupakan salah satu dampak negatif internet sebagai platform yang saat ini banyak digunakan.

Nah agar semakin mengenal, berikut merupakan ulasan lebih lengkap tentang cyber crime, contoh, serta jenis – jenis kejahatan cyber crime yang banyak ditemukan.

Pengertian Cyber Crime

Apa Itu Cyber Crime? Menurut Organization of European Community Development (OECD) cyber crime adalah semua bentuk akses ilegal terhadap suatu transmisi data.

Itu artinya, semua bentuk kegiatan yang tidak sah dalam suatu sistem komputer termasuk dalam tindak kejahatan.

Secara umum, *pengertian cyber crime* biasa diartikan sebagai tindak kejahatan di ranah dunia maya yang memanfaatkan teknologi komputer dan jaringan internet sebagai sasaran.

Seperti apa yang telah disebutkan, tindakan cyber crime ini muncul seiring dengan kian gencarnya teknologi digital, komunikasi dan informasi yang semakin canggih.

Contoh Kejahatan Cyber Crime

Agar lebih jelasnya, berikut ini merupakan contoh kasus cyber crime yang terjadi di Indonesia maupun di dunia.

1. Memalsukan Akun Facebook Seseorang

Salah satu contoh kejahatan cyber crime yang paling sering terjadi adalah pengkloningan akun facebook milik seseorang.

Tindakan ini marak terjadi kepada para public figur atau tokoh terkenal yang memiliki banyak pengikut.

Dengan banyaknya atensi yang diterima oleh akun kloningan, pemalsu biasanya akan semakin cepat mendapat korban.

Cyber crime model ini biasanya meminta bayaran uang dengan cara transfer ke rekening tertentu.

Jadi, jangan mudah percaya jika Anda dihubungi seseorang yang mengaku sedang membutuhkan bantuan.

2. Fenomena Ransomware WannaCry

Beberapa tahun lalu jagat digital sempat diramaikan dengan kemunculan virus komputer *Ransomware*

WannaCry yang mampu mengunci data komputer seseorang.

Untuk bisa membuka dan mengakses data, syarat yang harus Anda lakukan dengan membayar tebusan melalui e-wallet Bitcoin.

3. Catfishing di Dating App dan Media Sosial

Bedanya dengan cloning akun adalah catfishing menggunakan foto orang lain namun identitasnya merupakan identitas palsu.

Ini biasanya bisa Anda temukan di aplikasi dating atau di media sosial.

Nah, tujuan dari catfishing ini adalah sama-sama untuk menipu korban.

Kerugian yang ditimbulkan bisa mulai dari kerugian dalam bentuk uang dan barang.

4. Doxxing dan Cyberbullying

Doxxing yang berujung cyberbullying adalah hal yang sangat berbahaya.

Ini merupakan kegiatan pengambilan data pribadi dan menyebarkannya di internet.

Tujuan dari doxxing ini bermacam-macam, mulai dari sebagai gertakan, ancaman, mempermalukan hingga pemerasan.

Jenis–Jenis Cyber Crime

Setelah mengetahui tentang pengertian cyber crime dan contoh kasusnya, berikut ini merupakan jenis-jenis cyber crime yang banyak terjadi di dunia.

1. Pencurian Data

Aktivitas cyber crime yang satu ini biasanya dilakukan untuk memenuhi kepentingan komersil karena ada pihak lain yang menginginkan data rahasia pihak lain.

Tindakan ini tentu bersifat ilegal masuk ke dalam aktivitas kriminal karena bisa menimbulkan kerugian materil yang berujung pada kebangkrutan suatu lembaga atau perusahaan.

2. Cyber Terorism

Cyber terorism merupakan tindakan cyber crime yang sedang banyak diperangi oleh negara-negara besar di dunia, termasuk Indonesia.

Pasalnya, aktivitas cyber terorism kerap kali mengancam keselamatan warga negara atau bahkan stakeholder yang mengatur jalannya pemerintahan.

3. Hacking

Jenis cyber crime berikutnya adalah Hacking.

Tindakan berbahaya yang kerap kali dilakukan oleh para programer profesional ini biasanya secara khusus mengincar kelemahan atau celah dari sistem keamanan untuk mendapatkan keuntungan berupa materi atau kepuasan pribadi.

Jika menilik dari kegiatan yang dilakukan, hacking sebenarnya tidak selalu memiliki konotasi buruk karena ada pula hacker positif yang menggunakan kemampuannya untuk kegiatan bermanfaat dan tidak merugikan.

Misalnya, seorang hacker yang diberi tugas untuk melacak keberadaan seorang buronan atau hacker yang bekerjasama dengan pihak berwenang untuk memberantas aktivitas ilegal di ranah digital.

4. Carding

Carding adalah istilah yang digunakan untuk menyebut penyalahgunaan informasi kartu kredit milik orang lain.

Para carder (pelaku carding) biasanya menggunakan akses cartu credit orang lain untuk membeli barang belanjaan secara online.

Kemudian, barang gratisan tersebut dijual kembali dengan harga murah untuk mendapatkan uang.

Tindak kejahatan digital dengan cara carding biasanya kerap terjadi di luar negeri.

Sementara untuk pengguna di Indonesia angka kasus yang tercatat belum terlalu besar seiring masih minimnya pengguna kartu kredit yang gemar bertransaksi di dunia maya.

5. Defacing

Di antara tindakan cyber crime sebelumnya, Defacing bisa dibilang menjadi aktivitas kejahatan online yang paling ringan.

Hal tersebut salah satunya karena para pelaku deface biasanya menyasar website-website non-profit seperti situs pemerintahan, sekolah, atau universitas.

6. Cybersquatting

Istilah cybersquatting mungkin belum begitu familiar di kalangan pengguna di Tanah Air.

Wajar memang pasalnya tindakan penyerobotan nama domain sendiri memang memerlukan modal serta kejelian yang tidak dimiliki banyak orang.

Hasil cyber crime ini biasanya berupa uang tebusan yang nilainya tidak wajar.

7. Cyber Typosquatting

Hampir mirip dengan cybersquatting, tindakan cyber typosquatting sama-sama mengincar nama domain milik perusahaan terkenal untuk dijadikan sasaran.

Bedanya, aktivitas ini memanfaatkan kemiripan nama domain serta kelalaian pengguna yang jarang memeriksa ulang URL website perusahaan.

Salah satu tujuan dari cyber typosquatting adalah untuk menjatuhkan citra baik dari brand bersangkutan dengan cara melakukan tindakan penipuan atau hal-hal ilegal lain yang melanggar undang-undang.

8. Menyebarkan Konten Ilegal

Menyebarkan konten ilegal yang melanggar undang-undang menjadi kasus cyber crime paling banyak diperhatikan.

Pasalnya, aktivitas ini biasanya melibatkan tokoh terkenal atau konten yang mampu memancing kontroversi.

Beberapa contoh konten ilegal yang masuk dalam ranah cyber crime di antaranya adalah video porno, penjualan senjata api ilegal, jual beli narkotika, dan lain sebagainya.

9. Malware

Seperti yang sudah kami jelaskan di dalam artikel tentang **bahaya malware**, Anda harus lebih waspada jika tidak ingin komputer atau website mengalami kendala.

Secara umum, malware terdiri dari beragam jenis, ada virus, trojan horse, adware, worm, browser hijacker, dan lain sebagainya.

Metode Cyber Crime

1. Sniffing

Ini merupakan suatu metode yang mengancam keamanan jaringan siber.

Dalam konteks keamanan jaringan, serangan sniffing atau serangan sniffer sama dengan pencurian atau intersepsi data dengan mengumpulkan lalu lintas jaringan melalui

packet sniffer (aplikasi yang ditujukan untuk menangkap paket jaringan).

2. Destructive device

Tindakan kejahatan siber yang bertujuan untuk merusak device dengan menggunakan media sebuah virus yang disisipkan ke dalam sebuah program.

3. Password Cracker

Ini merupakan kegiatan meretas atau membobol password orang lain. Untuk melakukan hal ini, pelaku akan menggunakan software untuk membuka enkripsi program atau password.

4. Distributed Denial of Attacks (DDoS)

Serangan DDoS (Distributed Denial of Service) adalah jenis serangan jaringan terdistribusi.

Bentuk serangan ini memanfaatkan pembatasan kapasitas sumber daya jaringan, seperti infrastruktur yang mendukung situs web perusahaan.

Serangan DDoS akan membuat banyak permintaan ke sumber online yang ditargetkan untuk membanjiri kapasitas situs web untuk menangani banyak request dan mencegahnya bekerja dengan benar.

5. Spoofing

Spoofing adalah tindakan salah mengartikan pesan sumber yang tidak dikenal sebagai berasal dari sumber yang dikenal dan dapat dipercaya.

Dalam bentuk sederhana, spoofing bisa berupa komputer yang meniru alamat IP, Address Resolution Protocol (ARP), atau server Domain Name System (DNS), atau bahkan serumit komputer yang memalsukan alamat IP, ARP, atau server DNS.

Cara Penanggulangan Cyber Crime

1. Membuat Undang-Undang

Cara paling elegan agar tindakan cyber crime tidak semakin merajalela adalah dengan membuat peraturan yang dimasukkan kedalam Undang-undang.

Penegakan hukum nantinya bakal membuat para pelaku cyber crime berpikir panjang sebelum melakukan tindakan kriminal karena dasar hukumnya jelas.

Di Indonesia, aturan mengenai cyber crime saat ini menginduk pada UU ITE.

Namun, sayangnya pola penindakannya masih belum maksimal dan seringkali terkesan dipaksakan.

Penegakan hukum di ranah dunia maya memang masih abu-abu karena dokumen elektronik sendiri belum bisa dijadikan sebagai barang bukti oleh KUHP.

2. Membentuk Lembaga Penanganan Khusus

Anda tentu tidak asing dengan Divisi Cyber Crime Mabes Polri.

Nah, saat ini kita memerlukan lembaga khusus seperti itu untuk menangkal dan menyelidiki potensi terjadinya tindak kejahatan di ranah digital.

Beberapa negara tercatat sudah mulai menerapkan konsep ini dengan membentuk lembaga khusus yang menangani persoalan cyber crime.

Kendati demikian hal tersebut hanya akan efektif jika diterapkan oleh banyak negara, sehingga tidak ada celah bagi pelaku cyber crime dimanapun mereka berada.

3. Memperkuat Sistem

Pengamanan sistem menjadi benteng pertama yang bisa kita andalkan untuk menghindari potensi cyber crime.

Untuk mengamankan sistem secara mandiri Anda bisa menambahkan beberapa add ons seperti Sertifikat SSL pada website, antivirus komputer, hingga melakukan pengamanan fisik pada jaringan untuk memproteksi server.

Terlepas dari itu, jika Anda memiliki website bisnis, pastikan menggunakan layanan VPS Indonesia dari Qwords.com yang sudah dibekali berbagai teknologi masa kini.

Alhasil, kejahatan cyber crime seperti malware atau defacing lebih bisa diminimalkan.

13 Jenis Cyber Crime, Kejahatan Internet yang Merugikan

Cyber crime adalah kejahatan di dunia maya. Salah satu jenis kejahatan yang meningkat di tengah pandemi akibat perubahan gaya hidup masyarakat serba online.

Modus *cyber crime* macam-macam. Mulai dari pencurian data, pembobolan rekening, hingga minta-minta sumbangan atas nama korban pandemi.

Apa yang Dimaksud dengan *Cyber Crime*?

Cyber crime adalah tindakan ilegal yang dilakukan pelaku kejahatan dengan menggunakan teknologi komputer dan jaringan internet untuk menyerang sistem informasi korban.

Misalnya melakukan *hack* sosial media, membobol perangkat teknologi serta data korban. Lalu kemudian menyikat habis saldo rekening ataupun kartu kredit korban.

Cyber crime Indonesia diatur dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah menjadi UU Nomor 19 Tahun 2016. Jadi, belum ada UU *cyber crime* secara khusus.

Cyber crime termasuk dalam kategori perbuatan yang dilarang dalam UU ITE.

1. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun

2. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun 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 apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Jenis-jenis Kejahatan *Cyber Crime*

Ada beberapa jenis kejahatan *cyber crime* yang harus menjadi perhatian masyarakat, antara lain:

1. Kejahatan *Phising*

Phising adalah contoh *cyber crime* untuk melakukan penipuan dengan mengelabui korban. Umumnya aksi kejahatan ini dilancarkan melalui email maupun media sosial lain, seperti mengirimi *link* palsu, membuat *website* bodong, dan sebagainya.

Tujuannya mencuri data penting korban, seperti identitas diri, *password*, kode PIN, kode OTP (*one time password*) pada akun-akun keuangan, seperti *mobile banking*, *internet banking*, *paylater*, dompet digital, sampai kartu kredit.

2. Kejahatan *Carding*

Carding adalah jenis kejahatan dunia maya yang dilakukan dengan bertransaksi menggunakan kartu kredit milik orang lain. Jadi, setelah mengetahui nomor kartu kredit korban, pelaku kemudian berbelanja online dengan kartu kredit curian itu.

Nomor kartu kredit tersebut dicuri dari situs atau *website* yang tidak aman. Bisa juga diperoleh dengan cara membeli dari jaringan *spammer* atau pencuri data. Selanjutnya data kartu kredit itu disalahgunakan oleh *carder,* sebutan pelaku kejahatan *carding.*

3. Serangan *Ransomware*

Ransomware adalah *malware* atau *software* jahat yang bukan hanya bisa menginfeksi komputer, tapi juga menyandera data pengguna. Tindak kejahatan ini dapat menimbulkan kerugian besar bagi korbannya.

Pelaku akan meminta uang tebusan ke korban jika ingin *ransomware* dihapus atau dimusnahkan. Apabila korban tidak mengabulkan permintaan tersebut, pelaku tak segan-segan mengancam akan membuat data menjadi korup alias tidak bisa digunakan lagi.

4. Penipuan online

Penipuan online atau penipuan digital yang saat ini makin banyak modusnya. Di antaranya adalah modus penipuan berkedok foto selfie dengan KTP atau identitas diri.

Foto selfie bersama KTP biasanya menjadi salah satu syarat registrasi online akun keuangan, seperti dompet digital, paylater, pinjaman online, sampai daftar rekening bank online.

Bisa saja kamu terjebak aplikasi pinjaman online palsu yang dibuat sedemikian rupa. Kemudian oleh pelaku, data kamu dipakai untuk pencucian uang, dijual di pasar gelap, atau digunakan sesuka hati untuk pinjaman online ilegal.

5. SIM *Swap*

SIM *swap* adalah modus penipuan dengan mengambilalih nomor ponsel atau kartu SIM ponsel seseorang. Tujuannya untuk meretas akun perbankan seseorang.

Akibatnya, kartu SIM ponsel yang kemudian aktif dan berlaku adalah milik pelaku, bukan lagi punya korban. Oleh karena itu, jika ingin membuang kartu SIM lama, sebaiknya dipatahkan atau digunting agar tidak disalahgunakan orang lain.

6. Peretasan situs dan email

Kejahatan ini istilahnya *deface website* dan email. Yakni jenis kejahatan *cyber crime* dengan cara meretas sebuah situs ataupun email, serta mengubah tampilannya.

Dengan kata lain, penampilan *website* atau email kamu mendadak berubah akibat peretasan ini. Contoh, halaman situs bukan yang biasanya, jenis huruf ganti, muncul iklan tidak jelas, bahkan mencuri data yang kamu tidak menyadarinya.

7. Kejahatan *Skimming*

Jenis kejahatan *cyber crime* lain yang harus diwaspadai, yakni *skimming. Skimming* adalah kejahatan perbankan dengan cara mencuri data kartu debit atau kartu kredit untuk menarik dana di rekening.

Cara kerjanya membobol informasi pengguna memakai alat yang dipasang pada mesin Anjungan Tunai Mandiri (ATM) atau di mesin gesek EDC. Dengan teknik tersebut, pelaku bisa menggandakan data yang terdapat dalam pita magnetik di kartu kredit maupun debit.

Kemudian memindahkan informasi ke kartu ATM kosong. Akhirnya, pelaku bisa dengan mudah menguras saldo rekening nasabah.

Skimming dapat terjadi ketika kamu sedang transaksi belanja online. Saat kartu debit atau kartu kredit terhubung pada gawai, risiko terkena *skimming* menjadi lebih tinggi.

Ponsel atau laptop terkoneksi dengan internet sehingga memudahkan pelaku meretas atau mengambil data kartu kredit atau kartu debit. Terlebih jika menggunakan koneksi wifi publik. Jadi, pastikan setiap transaksi online pakai jaringan internet pribadi.

8. *OTP Fraud*

Pasti tahu dong OTP (*One Time Password*)? Kode sekali pakai yang sangat vital untuk keamanan bertransaksi.

Kode OTP ini ibarat kunci. Kunci akhir untuk bisa mengakses atau menyelesaikan transaksi keuangan. Jika kode 6 digit ini sampai diketahui orang lain, bisa berbahaya.

Saat ini, marak kejahatan pencurian kode OTP atau *OTP fraud*. Penyebab *OTP fraud* adalah *malware* atau semacam virus yang menyerang perangkat lunak.

Penyebab lainnya bisa juga melalui aplikasi, *social engineering* seperti via telepon, SMS, email. Contohnya lewat *call center* palsu.

9. Pemalsuan Data atau *Data Forgery*

Jenis kejahatan *cyber crime* Indonesia berikutnya adalah *data forgery*. Adalah kejahatan dengan memalsukan data atau dokumen penting melalui internet.

Biasanya kejahatan ini menyasar pada dokumen penting milik *e-commerce* atau penyedia situs belanja online. Seolah-olah terjadi salah ketik yang merugikan pengguna atau masyarakat.

10. Kejahatan konten ilegal

Divisi Hubungan Internasional Polri juga menyebut konten ilegal termasuk dalam jenis kejahatan *cyber crime*. Konten ilegal adalah kejahatan memasukkan data atau informasi yang tidak benar, tidak etis, melanggar hukum atau mengganggu ketertiban umum.

Sebagai contoh, berita bohong atau fitnah, pornografi, maupun informasi yang menyangkut rahasia negara, propaganda untuk melawan pemerintah yang sah.

11. "Teroris" Dunia Maya atau *Cyber Terorism*

Cyber terorism adalah kejahatan yang mengganggu, atau membuat kerusakan terhadap suatu data di jaringan komputer. Pelaku menawarkan diri kepada korban untuk memperbaiki data tersebut yang sudah disabotase dengan bayaran tertentu.

12. Mata-mata atau *Cyber Espionage*

Jenis kejahatan *cyber crime* yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer korban.

Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized.*

13. Menjiplak Situs Orang Lain

Kejahatan melanggar Hak Atas Kekayaan Intelektual (HAKI) orang lain di internet. Misalnya meniru tampilan situs orang lain secara ilegal, menyiarkan informasi yang merupakan rahasia dagang orang lain.

Selalu Jaga Kerahasiaan Data Kamu

Apapun bentuk atau jenis kejahatan *cyber crime* tidak dapat ditoleransi. *Cyber crime* bukan saja menimbulkan kerugian materiil, tetapi juga immaterial.

Untuk itu, pastikan kamu selalu menjaga kerahasiaan data pribadi. Hindari memposting data pribadi di media sosial, apalagi foto selfie dengan identitas diri. Jadilah pengguna internet bijak dan cerdas agar terhindar dari *cyber crime.*

Cyber Crime Meningkat Tajam di Masa Pandemi

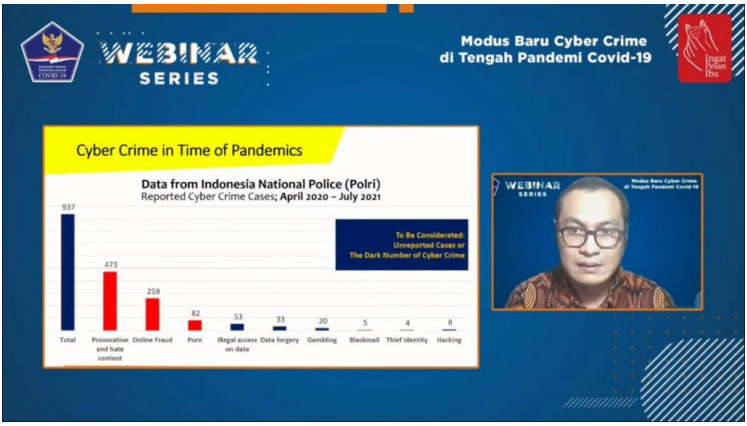
Faktanya bukan hanya kegiatan secara fisik saja yang terjadi bahkan *cybercrime* juga menjadi salah satu jenis kejahatan yang mengalami peningkatan cukup tinggi, modusnya juga kian beragam, seperti oknum yang meminta sumbangan dengan mengatasnamakan korban pandemi, pencurian data dan pembobolan rekening, hal ini merupakan hal yang harus di waspadai secara bersama mengingat tindak kejahatan ini tidak memandang bulu.

Cybercrime adalah segala aktivitas illegal yang digunakan oleh pelaku kejahatan dengan menggunakan teknologi sistem informasi jaringan komputer yang secara langsung menyerang teknologi sistem informasi dari korban. Namun secara lebih luas kejahatan *cyber* bisa juga di artikan sebagai segala tindak illegal yang didukung dengan teknologi komputer.

“Target pelaku adalah device atau hardware atau software atau juga data personal dari korban. Sifat dari *cybercrime* ini adalah baik pelaku maupun korbannya sama-sama *invisible* atau tidak terlihat, hal ini yang membuat jenis cybercrime ini punya kompleksitas sendiri. Pelaku potensial dari jenis *cybercrime* ini, dia bisa dari kelompok yang geologis ataupun kelompok yang berbisnis secara illegal dan individu tertentu” jelas Bhakti.

Menurut Bhakti, keuntungan pelaku di aktivitas *cybercrime* adalah yang pertama memungkinkan anonimitas jadi pelaku dengan lebih mudah menyembunyikan identitas mereka, kedua adalah ketika pelaku melaksanakan kejahatan diruang *cyber* ada jeda waktu yang memungkinkan pelaku lebih leluasa untuk menghilangkan barang bukti agar mengecoh dan mencegah respon dari upaya-upaya yang dilakukan oleh penegak hukum.

Pengguna internet baik di dunia maupun di Indonesia setiap tahunnya semakin meningkat, tentunya ada sisi positif dari jaringan internet yang tinggi, namun dari sisi negatifnya tentunya internet atau teknologi informasi ini menjadi *tools* baru yang digunakan oleh pelaku kejahatan untuk merugikan orang lain.



Sumber data : Kepolisian Republik Indonesia

Menurut data dari POLRI, bulan April 2020 sampai di bulan ini, setidaknya ada 937 kasus yang dilaporkan. Dari 937 kasus tersebut ada tiga kasus dengan angka tertinggi yaitu kasus *provocative, hate content and hate speech* yang paling banyak dilaporkan, sekitar 473 kasus. Kemudian disusul oleh penipuan *online* dengan 259 kasus dan konten porno dengan 82 kasus.

"Lalu mengapa angka kasus *provocative, hate content and hate speech* ini menjadi yang tertinggi, hal ini dipengaruhi oleh residues politik di Indonesia yang terjadi beberapa waktu lalu baik pemilihan daerah maupun pemilu nasional yang membelah masyarakat menjadi dua. Hal tersebut terbawa hingga saat ini dimana saat pandemi terjadi seharusnya masyarakat Indonesia bersatu untuk melawan wabah ini tetapi malah saling bertengkar dan menyalahkan satu sama lain" ujar Bhakti.

Ada kejahatan baru selama pandemi ini terjadi yaitu memanfaatkan barang dan alat kesehatan dengan menaikan harga diatas normal atau bahkan menimbunnya yang menjadikan kelangkaan di masyarakat umum. Selain itu juga informasi hoaks tentang pandemi Covid-19 yang disebar luaskan oleh beberapa tokoh dan kemudian ditangkap oleh polisi. Para pelaku ini memanfaatkan dan mengambil keuntungan dari kerentaan, ketidakberdayaan dan keterbatasan masyarakat selama pandemi ini terjadi.

Kejahatan siber atau kejahatan dunia maya

adalah kejahatan yang melibatkan komputer dan jaringan. Komputer mungkin digunakan untuk melakukan

kejahatan, atau menjadi target kejahatan. Kejahatan dunia maya dapat membahayakan keamanan dan keuangan seseorang.

Ada banyak masalah privasi seputar kejahatan siber ketika informasi rahasia dicuri atau diungkapkan, secara sah atau sebaliknya. Secara internasional, baik aktor pemerintah maupun non-pemerintah terlibat dalam kejahatan dunia maya, termasuk spionase, pencurian keuangan, dan kejahatan lintas batas lainnya. Kejahatan dunia maya yang melintasi perbatasan internasional dan melibatkan tindakan setidaknya satu negara bangsa kadang-kadang disebut sebagai perang siber. Warren Buffett menggambarkan kejahatan siber sebagai "masalah nomor satu umat manusia" dan "menimbulkan risiko nyata bagi kemanusiaan."

Sebuah laporan (disponsori oleh McAfee) yang diterbitkan pada tahun 2014 memperkirakan bahwa kerusakan tahunan pada ekonomi global akibat kejahatan siber mencapai $445 miliar. Sebuah laporan tahun 2016 oleh usaha keamanan siber memperkirakan bahwa kerusakan global yang terjadi sebagai akibat dari kejahatan dunia maya akan menelan biaya hingga $6 triliun per tahun pada tahun 2021 dan $10,5 triliun per tahun pada tahun 2025.

Sekitar $1,5 miliar uang hilang pada tahun 2012 karena penipuan kartu kredit dan debit daring di AS. Pada tahun 2018, sebuah studi oleh Center for Strategic and International Studies (CSIS), bekerja sama dengan McAfee, menyimpulkan bahwa hampir satu persen dari

PDB global, hampir $600 miliar, hilang karena kejahatan dunia maya setiap tahun. Laporan Risiko Global Forum Ekonomi Dunia 2020 mengkonfirmasi bahwa badan-badan kejahatan dunia maya yang terorganisir bergabung untuk melakukan kegiatan kriminal secara daring sambil memperkirakan kemungkinan deteksi, hingga kini penuntutan terhadap kejahatan siber kurang dari 1 persen di AS.

Jenis-jenis

Terdapat beberapa kejahatan dunia maya yang harus menjadi perhatian masyarakat sehingga tidak menjadi korban, berikut beberapa kejahatan dunia maya yang ada.

Kejahatan Pengelabuan

Pengelabuan merupakan cara untuk melakukan penipuan dengan maksud mencuri akun korban. Biasanya, pelaku menargetkan korban melalui email. Sehingga melalui email pelaku dapat mengambil alih akun dengan maksud tertentu. Pengelabuan juga diartikan sebagai upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan. Data yang dimaksud adalah data pribadi seperti nama, usia, alamat, serta data akun tertentu bahkan data finansial.

Penipuan kartu kredit

Penipuan kartu kredit merupakan istilah penyalahgunaan informasi kartu kredit milik orang lain. Para pelaku carding biasanya menggunakan akses kartu kredit orang

lain untuk membeli barang belanjaan secara online. Kemudian, barang tersebut dijual kembali dengan harga murah. Tindak kejahatan carding kerap terjadi di luar negeri, sementara di Indonesia angka kasus yang tercatat masih kecil.

Serangan Perangkat pemeras

Perangkat pemeras adalah software malware yang mengenkripsi file dan dokumen dari salah satu komputer hingga kepada seluruh jaringan, pelaku akan meminta tebusan pada korbannya untuk bisa mengakses lagi jaringan yang telah diambil alih. Perangkat pemeras juga didefinisikan sebagai malware yang menargetkan perangkat keras untuk mendapatkan informasi berharga pengguna serta mengenkripsi seluruh yang ditemukannya.

Penipuan online

penipuan online adalah penggunaan layanan internet atau software yang menggunakan akses internet untuk melakukan penipuan atau mengambil keuntungan dari korban. Metode dan alat yang digunakan untuk melakukan kejahatan sangat bervariasi, mulai dari software serta kerentanan pada hampir semua program dan aplikasinya.

SIM *Swap*

Kejahatan SIM Swap merupakan upaya pengambilalihan kartu SIM korban oleh oknum, sehingga kartu SIM yang dimiliki oleh korban tidak dapat digunakan sama sekali.

Di sisi lain, kartu SIM baru memiliki seluruh akses serta memperoleh manfaat dari fitur terkait, seperti halnya akses transaksi rekening bank korban.

Kejahatan *Skimming*

Skimming merupakan salah satu jenis penipuan yang masuk ke dalam metode pengelabuan. Cara kejahatan ini dilakukan dengan mencuri data penting orang lain, termasuk data bank seperti nomor rekening, data ATM seperti nomor kartu dan PIN, bahkan data kartu kredit seperti nomor dan jenis kartu serta PIN.Tujuan dari kejahatan *skimming* sendiri untuk mencuri informasi dari kartu debit atau kredit milik nasabah dengan menggunakan alat khusus bernama *Skimmer*. Sehingga *skimming* disebut pula sebagai kejahatan perbankan.

OTP Fraud

Kejahatan *On Time Password (OTP) Fraud* merupakan kejahatan yang dilakukan dengan cara peretasan atau pembajakan kode rahasia secara elektronik. Dengan membagikan kode rahasia OTP terhadap siapa pun secara elektronik, maka sama saja dengan memberikan kode rahasia milik korban kepada pelaku kejahatan.[24]

Pemalsuan Data

Pemalsuan data adalah data pemalsuan yang merupakan kejahatan dengan memalsukan data pada dokumen penting yang tersimpan sebagai *scripless* document melalui Internet. Tujuan dilakukannya kejahatan ini untuk

memalsukan data pada dokumen penting yang ada di internet. Dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.

Kejahatan konten ilegal

Konten ilegal adalah tindakan memasukkan data dan/atau informasi ke dalam internet yang dianggap tidak benar, tidak etis, serta mengganggu ketertiban umum bahkan melanggar hukum.

Terorisme siber

Terorisme siber merupakan aktivitas dan/atau metode yang digunakan oleh sejumlah jaringan atau kelompok teroris.

Pengintaian siber

Pengintaian siber merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan pemantauan atau menjadi mata-mata terhadap pihak lain, dengan cara memasuki sistem jaringan komputer pihak sasaran. Biasanya kejahatan ini ditujukan terhadap saingan bisnis yang dokumen atau data pentingnya tersimpan dalam suatu sistem yang terkomputerisasi.

Menjiplak Situs Orang Lain

Salah satu kejahatan dalam dunia maya adalah kejahatan melanggar Hak Atas Kekayaan Intelektual (HAKI) orang lain di internet. Salah satu contoh adalah melakukan peniruan terhadap tampilan situs orang lain secara ilegal, menyiarkan informasi yang merupakan rahasia dagang.

Pencegahan

Berikut adalah beberapa hal yang dapat dilakukan dalam upaya penanggulangan *cyber crime*

1. Mengamankan sistem.
2. Penganggulangan global.
3. Perlunya cyberlaw.
4. Perlunya dukungan lembaga khusus.

Sedangkan penanganan yang tepat untuk mencegah *cyber crime* terjadi pada pribadi dapat dilakukan melalui hal-hal berikut:

1. Lindungi gadget, komputer atau perangkat lain yang digunakan.
2. Jangan gunakan *software* bajakan.
3. Pasang perangkat lunak keamanan yang *up to date.*
4. Menggunakan *data encryption.*
5. Selalu miliki sikap waspada.
6. Selalu periksa data bank dan data kartu kredit secara teratur.
7. Rajin mengganti kata sandi.

8. *Backup* data-data secara rutin.
9. Jangan sembarang membagikan info pribadi.
10. Abaikan lampiran surat elektronik dan URL yang terindikasi mencurigakan.
11. Jangan langsung tergiur, gunakan waktu untuk berpikir lebih panjang dan matang.
12. Laporkan ke pihak yang berwenang.

DAFTAR PUSTAKA

https://www.seputarpengetahuan.co.id/2014/11/komputer-forensik-pengertian-dan-tujuan.html

https://www.cnnindonesia.com/nasional/20170405134633-12-205111/otak-pembobol-situs-tiketcom-ditangkap

https://www.labana.id/view/bedah-kasus-kopi-sianida-jessica-dari-sisi-digital-forensic/2016/10/20/?fullview

Information Security and Forensics Society :
http://www.isfs.org.hk
Ilmu Forensik :
https://id.wikipedia.org/wiki/Ilmu_forensik
UU ITE : https://id.wikipedia.org/wiki/Undang-Undang_Informasi_dan_Transaksi_Elektronik

https://money.kompas.com/read/2020/11/14/122726526/ojk-jamin-duit-tabungan-winda-akan-diganti-maybank-asalkan?page=all

https://www.cnbcindonesia.com/market/20201113135149-17-201646/maybank-siap-ganti-duit-winda-hotman-rp-22-m-uang-kecil

Sumber : https://mti.binus.ac.id/2019/04/05/forensic-dan-hukum-kejahatan-internet/

https://lms.onnocenter.or.id/wiki/index.php/Forensik#:~:text=Selaras%20dengan%20definisinya%2C%20secara%20prinsip,yang%20sah%20di%20pengadilan%3B%20dan

https://www.youtube.com/watch?v=Pfjjn0dk_iA

https://www.irondefencesecurity.ca/post/understating-the-utility-of-computer-forensics-today-and-it-s-impact

https://ternate.tribunnews.com/2020/05/04/3-orang-jadi-tersangka-ujaran-kebencian-terhadap-jokowi-dan-terawan-ratusan-akun-ig-segera-diblokir

https://www.youtube.com/watch?v=Pfjjn0dk_iA&ab_channel=NarasiNewsroom)

https://qwords.com/blog/pengertian-cyber-crime/

www.cermati.com/artikel/13-jenis-cyber-crime-kejahatan-internet-yang-merugikan

https://id.wikipedia.org/wiki/Kejahatan_siber

PENULIS BUKU DIGITAL FORENSIK

Muhammad Syarif Hartawan M.Kom MM
Universirtas Krisnadwipayana

Suhardjono S.Kom M.Kom
Universitas Bina Sarana Informatika

Ridwansyah, S.Kom, M.Kom
Universitas Nusa Mandiri

Verry Riyanto, S.Kom, M.Kom
Universitas Bina Sarana Informatika

Dr. Arman Syah Putra S.Kom MM M.Kom
Universitas Bina Nusantara