BAB III
KASUS KEJAHATAN PEMBOBOLAN ATM MELALUI TEKNIK *SKIMMING*

A. Kasus Pembobolan ATM Melalui Teknik *Skimming*

Dalam menjalankan aksinya para pelaku menggunakan teknik yang berbeda dan modus yang berbeda pula, berikut adalah beberapa kasus pembobolan ATM dengan menggunakan teknik *skimming*:

NO	KASUS	TEKNIK YANG DIGUNAKAN
1	Kasus di Denpasar, Bali. Tahun 2012. Dengan tersangka bernama: Zainal Abidin, I Putu Suniya Antara, Firdaus Theody.	Zainal Abidin bersama I Putu Suniya Adi Antara melakukan perbuatan tersebut pada saat dirinya bekerja sebagai Kapten di restoran Black Canyon Coffe ada beberapa customer yang berbelanja dan memesan makanan di restoran Black Canyon Coffe kemudian setelah coustemer selesai makan coustemer tersebut membayar dengan menggunakan kartu debit dan kredit selanjutnya Zainal Abidin dan I Putu Suniya Adi Antara akan menggesekan kartu tersebut ke card rider yang terdapat di Kasir restoran

		Black Canyon Coffe setelah Zainal Abidin dan I Putu Suniya Adi Antara menggesekan satu kali dan menggesekan kedua kalinya sehingga muncullah nomor kartu customer setelah muncul data-data coustemer selanjutnya Zainal Abidin dan Putu Suniya Adi Antara mencatat data-data yang berada di komputer tersebut dengan menggunakan kertas dan pulpen dan selanjutnya Zainal Abidin dan I Putu Suniya Adi Antara mengirim data tersebut menggunakan handphone milik Zainal Abidin kemudian data-data tersebut dikirim kepada Firdaus Theody dan setelah Zainal Abidin menyerahkan data-data para nasabah ke Firdaus Theody, Zainal Abidin dan I Putu Suniya Adi Antara mendapatkan imbalan berupa uang. Firdaus Theody semenjak bulan Desember 2010 merekrut atau mencari kasir-kasir karyawan yang bekerja di

		sebuah mall dan restouran di daerah Kuta Bali dan mengajarkan para kasir atau karyawan yang telah Firdaus Theody rekrut, bahwa apabila mereka melayani pembayaran dengan menggunakan kartu Debit atau kredit agar membuka Microsoft Word atau note pada kemudian kartu digesekkan kembali kepada mesin barcode magnetic reader maka data magnetic tersebut akan muncul pada file Microsoft Word atau Note Pad, kemudian apabila nasabah yang berbelanja dengan menggunakan debit card maka Firdaus Theody menyuruh untuk melihat dan mengingat nomor PIN nasabah yang berbelanja kemudian mencatatnya, selanjutnya file tersebut disimpan dalam bentuk file Microsoft Word kemudian disimpan dalam Flash Disc dan selanjutnya data tersebut diserahkan kepada Firdaus Theody dan apabila pada komputer kasir tempat

		bekerjanya tidak ada barcode magnetic reader maka Firdaus Theody mengajarkan dengan menggunakan skimmer (card device model MINI DX3), dimana setiap nasabah yang akan berbelanja cukup digesekkan ke dalam skimmer maka datanya akan terekam di skimer tersebut kemudian melihat dan mengingat PIN dari kartu debit yang digunakan untuk membayar selanjutnya mencatatnya untuk setiap transaksi kemudian setelah selesai skimmer tersebut diserahkan kepada Firdaus Theody untuk di buka dan datanya direkam. Atas data-data magnetic tersebut yang kemudian oleh Firdaus Theody jual kembali kepada RUSLI (DPO) dan ada juga yang oleh Firdaus Theody pergunakan untuk membuat kartu Debit dan kredit dengan cara data-data yang tersangka peroleh dari Zaenal Abidin, kemudian Firdaus Theody olah dengan

		cara pertama Firdaus Theody menginstal perangkat lunak (Software) MSR (Magnetik Strif Reader) 206 U dalam Laptop milik Firdaus Theody Kemudian software tersebut oleh Firdaus Theody dibuka program MAGNETIK STRIF READER / WRITER, kemudian data berupa angka – angka dan simbol yang Firdaus Theody peroleh dari Zainal Abidin yang didapat dari mengambil data nasabah yang berbelanja di Black Canyon, Firdaus Theody masukkan kedalam program tersebut selanjutnya Firdaus Theody menghubungkan alat ENCODE MSR 206 U dengan Laptop Firdaus Theody kemudian Firdaus Theody memberikan perintah pada program untuk menulis data kemudian menggesekkan kartu yang ada magneticnya sehingga data tersebut akan berpindah ke kartu magnetic yang Firdaus Theody gesekkan tersebut

		kemudian kartu tersebut dapat dipergunakan untuk melakukan transaksi keuangan seperti layaknya kartu Debit / kredit asli milik nasabah.
2	Kasus di Bali. Tahun 2016. Dengan tersangka bernama: Yonko Ivanov.	Dalam aksinya, pelaku melepas skimming angka-angka di mesin ATM yang biasa dipakai nasabah untuk memasukkan nomor PIN saat melakukan transaksi. Selanjutnya ia memasang alat perekam di bawah talang angka-angka tersebut, sehingga pada saat nasabah melakukan transaksi menekan tombol nomor PIN terekam oleh kamera yang telah dipasang pelaku. Setelah itu, tiga hari kemudian pelaku datang mengambil alat perekamnya tersebut lalu pelaku mengirimkan data-data nasabah kepada rekannya yang berada di Bulgaria.

3	Kasus di beberapa Rumah Sakit besar yang berada di Bandung dan Jakarta. Tahun 2014. Dengan tersangka bernama: Khor Chee Sean, Saw Hing Woo, Teh Chen Peng, Lee Chee Kheng, Ong Lung Win, dan Ooi Choo Aun yang semuanya berasal dari Malaysia.	Teoh Chen Peng dan Ong Lung Win mengantar Lee Chee Keng , Khor Chee Sean dan Saw Hong Woo ke tempat pemasang alat skimer di mesin ATM dan alat kamera yang berada di Rumah Sakit, tapi Teoh Chen Peng dan Ong Lung Win menunggu di tempat yang agak jauh dari tempat mesin ATM tersebut yaitu di sekitar RS Pondok Indah Jakarta, sekitar RS 12 Husada Jakarta dan sekitar RS Pantai Indah Kapuk Jakarta serta tempat lainnya (kemungkinan di sekitar RS Bormeus, Bandung). Setelah selesai melakukan pekerjaannya Lee Chee Keng, Khor Chee Sean dan Saw Hong Woo bertemu lagi dengan Teoh Chen Peng dan Ong Lung Win, selanjutnya mereka pulang ke Hotel lagi, ini dilakukan hampir tiap hari. Ooi Choo Aun, tgl 11 Februari 2014 bergabung dengan Teoh Chen Peng dan Ong Lung Win serta para saksi serta saudara

		MOW SHING XIANG (DPO) dalam hotel yang sama di Jakarta. Ooi Choo Aun, Teoh Chen Peng dan Ong Lung Win membantu saudara MOW SHING XIANG (DPO) memasukan data-data para nasabah kedalam kartu-kartu yang sudah disediakan oleh saudara MOW SHING XIANG (DPO) atau penggandaan kartu, sewaktu berada di Hotel. Pada tgl 17 Februari 2014 Ooi Choo Aun, Teoh Chen Peng dan Ong Lung Win bersama Lee Chee Keng, Khor Chee Sean dan Saw Hong Woo bersama saudara MOW SHING XIANG (DPO) pulang ke Malaysia. Pada tgl 21 Februari 2014 Teoh Chen Peng dan Ong Lung Win bersama Lee Chee Keng bersama MOW SHING XIANG (DPO) datang ke Medan dan menginap di Hotel Swiss Bellin Medan. Selanjutnya pada tgl 22 Februari 2014 Ooi Choo Aun bersama Khor Chee Sean dan Saw Hong Woo

		datang ke Medan dan bergabung dengan Teoh Chen Peng dan Ong Lung Win bersama Lee Chee Keng bersama MOW SHING XIANG (DPO), juga menginap di Hotel Swiss Bellin Medan. Sejak tgl 21 Februari 2014 s/d 27 Februari 2014 Ooi Choo Aun, Teoh Chen Peng dan Ong Lung Win bersama Lee Chee Keng, Khor Chee Sean dan Saw Hong Woo, dalam melakukan pengambilan atau penarikan uang menggunakan kartu-kartu yang sudah berwarna kuning, hijau, biru dan emas berikut No.Pin nya, telah disediakan oleh saudara MOW SHING XIANG (DPO). Ketiga tersangka dan Lee Chee Keng, Khor Chee Sean dan Saw Hong Woo diberi oleh saudara MOW SHING XIANG 10 kartu atau ada yang lebih. Pengambilan atau penarikan uangnya dilakukan kurang lebih 5 – 6 kali, hampir setiap hari, di mesin ATM Hotel Swiss Bellin Medan, di mesin

		ATM Yuki simpang Raya Medan, di mesin ATM Hotel Garuda Medan, di mesin ATM Merdeka Walk Medan dan di mesin ATM Merdeka Plaza Medan serta di tempat lain di wilayah Medan.
4	Kasus yang terjadi di Bandung, Tahun 2017. Direktorat Reserse Kriminal Khusus Polda Jabar mengungkap praktik sindikat peretas atau hacker kartu kredit. Sebanyak 18 orang berhasil diamankan yang kebanyakan dari mereka masih remaja. Bahkan satu di antaranya yakni seorang perempuan.	Menurut Direskrimsus Polda Jabar Kombes Pol Samudi, pelaku ini diamankan di salah satu hotel di Kota Bandung tempat aksi mereka dilakukan. Pihak hotel merasa curiga dengan transaksi yang diduga bukan menggunakan data pribadi. Kecurigaan itulah membuat pihak hotel melaporkan ke kepolisian. Setelah ditelusuri, diketahui para pelaku memang merupakan sindikat pembobol dan peretas kartu kredit. Dari tangan para tersangka diamankan berbagai barang bukti seperti laptop, mesin skimmer, CPU, kartu perdana dan masih banyak lagi. Direktorat Reserse Kriminal Khusus Polda Jabar mengungkap

		praktik sindikat peretas atau hacker kartu kredit. Sebanyak 18 orang berhasil diamankan yang kebanyakan dari mereka masih remaja. Bahkan satu di antaranya yakni seorang perempuan. Modusnya menggunakan model spam. Yakni dengan memanipulasi halaman web, targetnya untuk meminta rincian data pribadi calon korban. Ada juga yang modusnya menawarkan jual beli barang dari situs underground. Dengan meretas kartu kredit itu, para pelaku bisa dengan leluasa menggunakannya seperti untuk reservasi pembelian tiket pesawat, reservasi hotel hingga belanja online.

Berdasarkan tabel diatas, pelaku menggunakan modus dan teknik yang sangat cerdik dan para pelaku juga merekrut orang lain agar pelaku semakin mudah dalam melakukan aksinya. Pada kasus pertama, pelaku merekrut karyawan cafe kopi yang berada di Bali kemudian pelaku tersebut melakukan pelatihan kepada karyawan tersebut agar bisa

mengikuti instruksi pelaku dengan baik, pada kasus pertama maupun yang kasus yang ke dua mereka mengincar kota Bali. Karena, banyaknya turis mancanegara yang berkunjung ke Bali menjadi alasan utama mengapa para pelaku mengincar kota tersebut. Selain itu pelaku terkadang mengincar restoran ataupun cafe yang memiliki nilai jual yang tinggi, karna bagi mereka dengan cafe yang cukup mewah maka pengunjung yang datang pasti akan memiliki uang yang banyak pula. Pada kasus pertama, setelah mendapatkan data dari ATM nasabah pelaku menjual kembali data tersebut kepada orang lain dan data tersebut ada pula yang digunakan sendiri oleh pelaku.

Pada kasus ke dua, pelaku hanya bertugas untuk melakukan perekaman data yang terdapat pada ATM korban lalu pelaku mengirim data-data tersebut kepada rekannya yang berada di Bulgaria untuk diolah agar uang korban bisa diambil oleh pelaku lain yang berada diluar negara Indonesia.

Dalam kasus ke 3, pelaku mengincar beberapa rumah sakit yang ada di kota-kota besar. Dalam kasus ke 3 ini pelaku memang tidak mengincar kota dengan tingkat kunjungan wisatawan yang tinggi seperti pada kasus ke 1 dan 2, namun mereka melakukan aksinya di rumah sakit secara acak para pelaku tersebut sudah mengetahui masing-masing tugasnya sehingga dalam aksinya tidak semua pelaku mendatangi ATM yang berada di rumah sakit namun sebagian dari pelaku menunggu di hotel untuk mengolah data yang telah didapat oleh pelaku yang bertugas dilapangan. Pelaku pada

kasus ke 3 ini menggunakan ATM palsu untuk memasukan data yang sudah diperoleh agar ATM yang palsu tersebut bisa digunakan oleh para pelaku. Para pelaku selalu berpindah-pindah tempat tinggal maupun lokasi ATM yang dijadikan target oleh pelaku.

Pada kasus ke empat para pelaku sudah meninggalkan modus dengan melakukan pengcopyan data secara langsung melalui ATM, mereka tidak lagi harus repot pergi ke mesin ATM. Mereka menggunakan modus spam ke email korban sehingga nantinya korban sendiri yang akan mengisi data pribadi pada web yang dibuat oleh pelaku, semakin canggihnya teknologi maka akan semakin pintar pula para pelaku dalam membuat modus-modus baru dalam kejahatan skimming ini.

B. Hasil Wawancara dengan Pihak Bank dan Kepolisian

Wawancara dengan Pak Guntur sebagai pegawai salah satu Bank di Wilayah Jatibarang, Kabupaten Indramayu. Wawancara ini dilakukan pada tanggal 18 Maret 2017, pukul. 13.30 WIB, dicafe milik pak Guntur.

Bagaimana cara membobol ATM dengan modus *skimming* tersebut?

Pada intinya pelaku hanya perlu dua hal yang pertama duplikat kartu ATM dan PIN ATM nasabah sendiri. Kedual hal tersebut diperoleh oleh pelaku secara tidak langsung dari tangan nasabah sendiri sewaktu nasabah menggunakan *Automatic Teller Machine* (ATM). Secara diam-diam pelaku memasang alat tertentu pada mesin ATM tersebut sebelum calon korban menggunakannya. Kemudian pelaku meng-copy data kartu ATM nasabah, dengan cara menempelkan alat skimmer pada tempat nasabah

memasukan kartu ATM bentuk dari alat skimmer ini hampir menyerupai bagian dari mesin itu sendiri, sehingga tampak asli dan tidak membuat nasabah curiga.

Saat nasabah hendak menggunakan ATM dan mulai memasukkan kartu, saat itulah skimmer bekerja. Alat tersebut bisa membaca data yang tersimpan pada kartu melalui *magnetic stripe* (pita hitam yang terdapat pada bagian belakang kartu) kemudian menyalin dan menyimpannya. Setelah mengumpulkan beberapa salinan data, proses selanjutnya pelaku datang kembali untuk mengambil skimmer dan mulai menggandakan kartu. Tahap ini dilakukan manual namun, tergantung seberapa canggih alat skimmer yang digunakan oleh pelaku. Karena, alat skimmer sendiri ada yang bisa mengirimkan data secara otomatis melalui pesan singkat di handphone dan ada yang tidak.

Bagaimana pelaku bisa mengetahui nomer *Personal Identity Number* (PIN) ATM nasabah?

Sejauh yang saya tahu ada 3 cara yang bisa pelaku lakukan, yang pertama pelaku memasang kamera pengintai ukuran kameranya jauh lebih kecil dari kamera *Closed Circuit Television* (CCTV) yang dipasang ditempat yang sekiranya bisa merekam gerakan jari saat anda mengetik PIN. Yang kedua pelaku memasang papan tombol palsu yang dipasang di atas papan ketik yang asli sehingga saat anda mengetik PIN papan ketik palsu tadi merekam dan mencatatnya. Yang ketiga, alat skimmer yang canggih tidak

hanya dapat meng-copy data, tapi juga dapat menyimpan PIN yang nasabah masukan.

Apa solusi keamanan ATM dari pihak bank?

Sebenarnya kami selaku pihak bank sudah melakukan edukasi kepada para nasabah kami, pada saat nasabah akan membuat kartu ATM yang baru kami selalu melakukan edukasi mengenai apa saja yang harus dihindari dan apa saja yang harus menjadi perhatian khusus bagi para nasabah agar terhindar dari hal-hal yang tidak diinginkan. Setiap pihak keamanan atau *security* selalu kami beri arahan agar selalu memberikan edukasi kepada para nasabah penggunakan ATM. Selain itu, kami juga melakukan cara dengan melepas penutup yang ada pada papan ketik di setiap mesin ATM bank kami karena, kami sadar bahwa penutup papan ketik tadi sudah dimanfaatkan oleh para pelaku kejahatan.

Bagaimana cara agar terhindar dari kasus *skimming* tersebut?

Ada beberapa cara agar nasabah bisa terhindar dari kejahatan *skimming* ini, yang pertama adalah sebelum menggunakan ATM amati dan teliti mesin ATM terlebih dahulu dari mulai papan ketik atau lubang tempat memasukan kartu ATM, jika terdapat bagian yang mencurigakan atau terlihat rusak lebih baik tinggalkan mesin ATM tersebut lalu nasabah bisa menghubungi bank yang bersangkutan. Yang kedua, pakailah mesin ATM yang terdapat kamera pengintai yang dipasang oleh pihak bank. Yang ketiga, pilihlah ATM yang lokasinya ramai seperti mesin ATM yang berada didepan bank atau yang terdapat penjagaan satpam. Yang keempat,

saat menginput PIN selalu tutupi dengan menggunakan tangan atau bisa juga dengan badan mendekat ke papan ketik dan punggung membungkuk. Yang kelima, aktifkan selalu SMS/Email *banking* yang terdapat pada *handphone* nasabah dan cek saldo secara berkala jika terjadi pengurangan saldo yang bukan dari transaksi nasabah segera laporkan kepada pihak bank dan apabila terjadi transaksi pendebetan di rekening nasabah yang bukan dilakukan oleh nasabah sendiri dihimbau untuk menghubungi pihak bank untuk melaporkan transaksi yang mencurigakan tersebut, dan dihimbau untuk segera memblokir kartu ATM dan menghapus semua *e-banking* yang teregister di kartu ATM.

Wawancara dengan AKP Wisnu Perdana Putra, S.H.,S.LK.,M.M sebagai kanit unit *cyber crime* di Kepolisian Daerah Jawa Barat, Bandung. Wawancara ini dilakukan pada tanggal 29 Maret 2017, pukul. 10.20 WIB. Bertempat di bagian Kriminal Khusus Kepolisian Daerah Jawa Barat.

Apakah dari tahun ke tahun teknik *skimming* yang digunakan oleh pelaku selalu sama?

Pada intinya alat skimmer memilik dua versi, ada yang namanya MSR (kartu yang memiliki pita magnetik) sekarang hampir semua kartu dari mulai ATM, kartu kredit ataupun KTP yang dipake bukan lagi pita magnetic untuk menyimpan semua data tapi menggunakan chip. Memang dulu teknik *skimming* ini masih menggunakan peng-copyan data melalui strip magnetik yang terdapat pada kartu, pelaku biasanya membeli kartu dari para pencopet atau dengan modus ganjal ATM kemudian pelaku

mengcopy data yang terdapat pada strip magnetic kartu tersebut. Untuk modus sekarang para pelaku *skimming* tidak lagi membutuhkan kartu kredit fisik karena, sekarang data dari kartu kredit itu sudah bisa dibeli dengan bebas di pasar illegal semua data kartu kredit diseluruh dunia ada disitu dari yang memiliki saldo ratusan juta hingga miliaran rupiah tersedia di forum atau pasar tersebut. Sekarang banyak hotel yang menggunakan kartu untuk membuka pintu kamar atau kartu member sebuah club mobil atau motor yang terdapat *strip magnetic* hitam dibelakangnya sehingga pelaku cukup mudah untuk membeli kartu yang sejenis dengan ATM tadi, karna pada dasarnya data kartu yang dibeli dari pasar gelap tersebutlah yang paling penting.

Jadi, modus *skimming* yang digunakan saat ini oleh para pelaku. Pertama adalah membeli data kartu kredit lalu *injeck* kartu pada tahap *injeck* inilah peran skimmer, *chip read/write* dan *print card* agar terciptalah ATM palsu dengan data dari nasabah yang dibeli dari pasar gelap tadi pada jaman sekarang ini semua bahan yang dibutuhkan sudah dijual di pasar Indonesia. Modus yang kedua adalah dengan teknik spam ke email dengan cara meminta kepada korban untuk memasukan data pribadi dari mulai data pribadi bahkan data bank itu sendiri setelah pelaku mendapatkan data korban lalu pelaku *injeck* data tersebut ke kartu yang kosong.

Apakah pelaku selalu menggunakan hasil *skimming* dengan cara mengambil uang lewat ATM?

Biasanya pelaku menggunakan hasil dari *skimming* dengan belanja online di situs-situs yang ada di internet. Misalnya dengan membeli tiket konser, tiket pesawat, tiket hotel atau membeli barang seperti *handphone* dan sebagainya para pelaku ini jarang sebenarnya mengambil uang secara langsung di ATM karena ada kelemahan yaitu ketika kartu di read di mesin ATM tidak akan terbaca oleh mesin ATM sehingga para pelaku lebih memilih untuk membelanjakan uang tersebut di mall-mall besar dengan menggesekkan ke mesin ECD (*Electronic Data Capture*) atau yang lebih dikenal dengan ATM Mini adalah Mesin yang berfungsi sebagai sarana penyedia transaksi dan alat pembayaran yang penggunaannya dengan cara memasukkan atau menggesek kartu ATM. Karena, tidak semua kasir yang ada di mall itu mengerti cara membaca suatu kartu debet atau kredit.

Apakah data korban yang diambil oleh pelaku masih bisa digunakan oleh korban itu sendiri selaku pemilik asli dari data tersebut?

Biasanya bank itu mempunyai keamanan sendiri, salah satunya adalah *one time password* cara kerjanya adalah jika ada transaksi dengan jumlah uang diatas yang telah ditentukan oleh bank maka memerlukan *one time password* atau harus memasukan kode yang telah dibuat oleh pemilik asli dari kartu ATM tersebut. Sehingga para pelaku ini lebih suka berbelanja online dibanding mengambil uang secara langsung di ATM.

Bagaimana pertanggungjawaban pidana terhadap pelaku *skimming* ATM?

Dalam pidana murni pelaku bisa jerat dengan pasal pencurian atau penipuan, serta ancaman hukumannya sendiri 12 tahun namun ini delik aduan sehingga yang merasa dirugikan harus melapor. Dalam pasal 30,31, dan 32 Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juga merupakan delik aduan. Kita dari pihak cyber crime Kepolisian Daerah Jawa Barat pernah melakukan kerja sama dengan interpol Jakarta dan menangkap pelaku *skimming* di hotel Cimbuluit Bandung dan sampe sekarang para pelaku tersebut tidak bisa kita tahan karna tidak ada jawaban ketika kami mengirimkan data-data dari pelaku sehingga kami tidak bisa membuat laporan dan pelaku tersebut kita bebaskan dengan pengawasan.

Apa saja kesulitan dari pihak kepolisian dalam menangani kasus *skimming*?

Kendala utama kami adalah karna dalam kasus ini merupakan delik aduan dalam artian yang dirugikan yang harus melapor, pihak bank juga tidak bisa melapor karna yang dirugikan bukan pihak bank yang mempunyai uang kan nasabah itu sendiri bukan bank.

Pelaku sekarang memilih negara yang tidak mempunyai kerjasama politik dengan Indonesia bila tidak ada kerjasama maka kami pun tidak bisa bekerja sama dengan pihak kepolisian di negara yang bersangkutan sehingga kami kesulitan dalam menangani kasus ini karena pada dasarnya harus ada laporan dulu baru kami proses, mangkannya pelaku ini jarang

bisa tertangkap kalaupun tertangkap yaitu pelaku yang mencuri data dari korban sekaligus menjual barang-barang hasil dari kejahatan tadi.

Kemudian Jaksa dan Hakim kadang tidak mengerti mengenai kasus *skimming* ini dan pasal yang dikenakan, akhirnya kami juntokan dengan pidana murni agar Penuntut Umum dan Hakim mengerti. Penuntut Umum dalam menentukan rencana tuntutan harus membaca resume yang penyidik berikan, Penuntut Umum kebanyakan tidak mengerti mengenai istilah ITE bila ada junto pidana murni maka Penuntut Umum langsung mengerti.

Anggaran penyidikan menjadi kendala lain, dalam satu tahun kita unit *Cyber Crime* diberikan anggaran penyidikan sebesar 80 juta dalam satu kasus prostitusi online saja kita sudah menghabiskan dana sebesar 80 juta. Sebenarnya untuk menutupi anggaran penyidikan yang habis tadi kita mempunyai penyerapan anggaran dari sektor lain namun akan membutuhkan waktu untuk mencairkan dana tersebut.