

HASIL WAWANCARA DENGAN AKBP AUDIE LATUHERY KASAT CYBERCRIME
DIT RESKRIMSUS POLDA METRO JAYA

1.	<p>Bagaimanakah proses pemeriksaan kasus yang dilakukan polisi setelah adanya pengaduan dari masyarakat?</p> <p>Setelah adanya pengaduan dari masyarakat (korban) polisi langsung mengadakan proses pemeriksaan. Dimulai dari diterimanya pengaduan, kemudian masyarakat membuat laporan atas kejadian yang dialaminya setelah itu Sentra Pelayanan Kepolisian yang menampung laporan tersebut akan menyerahkan laporan tersebut ke bagian kriminal khusus kemudian oleh Direktur akan mendisposisikan laporan tersebut ke bagian Divisi <i>cyber crime</i> yang menangani kasus tersebut.</p>
2.	<p>Sekarang ini, angka kejahatan pencurian data melalui internet melambung tinggi sehingga meresahkan masyarakat. Masyarakat yang menjadi korban juga enggan untuk melapor kepada polisi dengan berbagai macam alasan. Apakah kepolisian dapat bertindak tanpa adanya pengaduan dari pihak korban dengan adanya alasan untuk kepentingan masyarakat?</p> <p>Bisa, pelaku yang ditemukan oleh polisi bisa ditangkap dan diproses secara hukum.</p>
3.	<p>Berdasarkan penanganan kasus pencurian data melalui internet yang dilakukan oleh satuan unit cyber crime, modus apa yang sering dilakukan oleh pelaku?</p> <p>Ada beberapa modus pencurian data melalui internet salah satunya adalah dengan teknik <i>phishing</i>. Yaitu metode peniuan terhadap pengguna internet dengan melakukan pengiriman e-mail palsu yang seolah-olah berasal dari sumber yang dapat dipercaya. Isi <i>e-mail</i></p>

	<p>tersebut biasanya berusaha mencuri identitas pengguna dengan motif adanya pembaruan data atau semacamnya. Ada pula teknik pencurian data melalui internet yaitu pelaku berusaha membuat pengguna mengunjungi situs yang salah sehingga memberikan informasi rahasia kepada pihak yang tidak berhak. Untuk melakukan tehnik ini pelaku umumnya membuat situs yang mirip namanya dengan nama <i>server</i> asli. Misalnya www.bankxxx.com merupakan situs yang asli, maka hacker akan membuat situs bernama www.bank_xx.com, www.bankxxx.org, www.xx-bank.com, www.bankxxx.co.id. Dengan demikian ketika pengguna membuka alamat yang salah, ia akan tetap menduga ia mengunjungi situs bankxxx yang benar. Ketika korban Log in dia akan memasukan data pribadi miliknya dia sendiri disinilah terjadi pencurian data. Atau pengguna dikirim <i>link</i> dari <i>server</i> bankxxx (yang palsu) dan situs tersebut mirip dengan situs aslinya, ketika muncul menu agar pengguna memverifikasi atas penggunaan kartu atmnya seketika itu terjadilah pencurian data ketika pengguna memasukan data pribadinya.</p>
4.	<p>Apakah pihak kepolisian mempunyai kesulitan dalam menangani kasus pencurian data melalui internet? Bila ada faktor-faktor apa saja yang menyebabkan polisi untuk menangani?</p> <p>Tergantung pada kasusnya, tempus, locus dan korban, faktor itulah yang akan mempengaruhi proses penyidikan dalam kasus ini.</p> <p>Tindak pidana pencurian data melalui internet merupakan <i>cyber crime</i> yang memiliki tingkat kesulitan yang tertinggi. Karena harus membuktikan sebuah data yang bersifat maya atau digital berbeda dengan data yang bersifat fisik yang memang sudah jelas.</p> <p>Kesulitan juga didapat dari korban ketika korban itu sendiri enggan untuk memberikan data-data yang dicuri dengan alasan <i>privacy</i> karena polisi butuh data tersebut untuk dijadikan bukti yang mendapat mendukung proses sidik.</p>

5.	<p>Bagaimana tindakan polisi dalam melakukan pencarian pelaku setelah adanya pengaduan dari korban?(karena bisa di bilang dunia maya seperti internet sangat luas dan tidak terjangkau</p> <p>Tidak masalah, setiap kejahatan pasti meninggalkan jejak, walaupun di dunia maya sekalipun. Ada proses input dan output artinya ada sumber dan sampai tujuan mana, itulah yang menjadi petunjuk kami dalam memecahkan kasus ini. Setiap kejahatan pasti meninggalkan jejak.</p>
6.	<p>Dalam proses penyidikan kasus, biasanya kepolisian bekerja sama dengan pihak atau instansi apa dan membantu dalam hal apa?</p> <p>Dalam menangani kasus tindak pidana pencurian data melalui internet ini pihak Kepolisian biasanya bekerja sama dengan para ahli di bidang IT seperti ahli dari Kemkominfo dan juga para ahli pidana. Hal ini perlu karena dalam menangani kasus ini perlu pengkaitan antara bidang IT dan ilmu pidana, dan juga mengingat kasus pencurian data melalui internet ini memiliki tingkat kesulitan tertinggi dan memakan waktu yang lama dalam proses penyidikannya. Yakni bagaimana membuktikan sebuah data yang bersifat digital atau maya, berbeda dengan data yang berwujud fisik yang memang sudah jelas. Pihak kepolisian juga bekerja sama dengan pihak bank yang mau menjadi saksi apabila dalam kasus pencurian data nasabah.</p> <p>Pihak kepolisian juga bekerja sama dengan para akademisi ahli telematika dari universitas salah satunya adalah Univesitas Indonesia serta peminjaman fasilitas laboratoriumnya dan juga dalam penganalisaan barang bukti.</p>

7	<p>Apakah pasal 32 ayat (2) UU ITE dapat dijerat kepada pelaku tindak pidana pencurian data melalui internet?</p> <p>Bisa, pada dasarnya pasal tersebut digunakan untuk menjerat pelaku tindak pidana pencurian data baik yang dilakukan secara manual yaitu mengambil data tanpa menggunakan internet contohnya mengambil flashdisk kemudia data itu dipindahkan ke komputer atau media penyimpanan lain milik pelaku atau pencurian data melalui internet. Dan pasal itu pernah kami gunakan untuk menjerat pelaku.</p>
8.	<p>Berdasarkan penanganan dari pihak kepolisian selama ini data apa saja yang biasa dicuri oleh pelaku?</p> <p>Pada dasarnya data itu ada dua macam, yakni data yang bersifat pribadi dan data yang bersifat publik. Data yang bersifat pribadi adalah data yang bersifat <i>privacy</i> bagi si pemilik, contohnya seseorang yang menyimpan data-data catatan yang menyangkut kebiasaan pribadinya atau berkaitan dengan pekerjaannya,dll.</p> <p>Sedangkan data publik adalah data-data yang memang bisa diketahui oleh umum dan dapat dimanfaatkan oleh masyarakat, seperti data-data pemerintah. Hal ini juga bisa menjadi suatu permasalahan jika data itu dimanfaatkan secara tidak benar oleh pihak-pihak yang tidak bertanggung jawab. Data yang dimiliki oleh suatu badan usaha merupakan data publik, yang dimana juga sering terjadi penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab, motifnya adalah mencuri data perusahaan karena persaingan usaha.</p>

9.	<p>Dalam hal penyidikan biasanya barang bukti apa saja yang ditemukan?</p> <p>Copy dari data korban, print out e-mail, bila dalam perusahaan misalnya daftar penawaran suatu produk, faktur pengeluaran, nota kerja sama antara perusahaan yang satu dengan yang lain.</p>
10.	<p>Dalam kasus pencurian data melalui internet ini, menurut kepolisian barang-barang apa saja yang dapat dijadikan alat bukti yang sah?</p> <p>Berdasarkan pasal 184 KUHP bisa dari keterangan saksi, data-data <i>print-out</i> yang kemudian ditafsirkan kedalam surat yang dimana tekniknya dibantu oleh para ahli, juga dari forensik yang memang khusus menangani kejahatan <i>cyber crime</i> ini.</p>
11.	<p>Selama unit cyber crime menangani kasus ini, menurut pengakuan tersangka apa yang menyebabkan mereka melakukan tindak pidana?</p> <p>Faktor ekonomi menjadi merupakan alasan yang paling sering dijadikan pelaku sebagai motivasi dalam melakukan tindak pidana ini.</p> <p>Kemudian alasan kepuasan juga dijadikan motivasi dalam melakukan tindak pidana ini, karena para pelaku atau bisa disebut <i>hacker</i> selalu ingin menguji seberapa jauh kemampuannya berselancar di dunia maya dan juga dalam menjebol sistem pengamanan suatu komputer.</p>
12.	<p>Sebelum adanya Undang-Undang ITE, dalam menangani tindak pidana pencurian data melalui internet, pihak kepolisian menggunakan UU apa saja yang dapat menjerat pelaku tindak pidana sehingga pelaku tindak pidana memenuhi unsur-unsur tindak pidana pencurian data melalui internet?</p>

	<p>Sebelum adanya Undang-Undang ITE, dalam menangani tindak pidana pencurian data melalui internet, pihak kepolisian menggunakan Kitab Undang-Undang Hukum Pidana dalam menjerat pelaku. Pasal yang biasa yang dipakai adalah pasal 362 KUHP, 363 KUHP (disertai merusak atau menjebol sistem pengamanan).</p>
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------