Menelusuri Jejak Forensik Dari Beberapa Kasus
Sabtu, 8 Agustus 2015 | 22:46:29 WIB | **Endang Kurniawan**

Cybercrimes always have cybertrails. Di era serba digital seperti sekarang ini, setiap kasus pasti memiliki jejak digital dan bisa dilacak.
Kasus pembunuhan aktivis HAM (Munir), pembunuhan David Hartanto Widjaja (mahasiswa NTU Singapura), kecurangan pajak, kasus Bank Century, hingga tersebarnya video biru artis papan atas Indonesia merupakan beberapa contoh kasus yang mengandalkan barang bukti digital dalam penyelesaiannya.

Tak banyak orang yang menganggap barang digital itu penting. Apalagi untuk orang awam yang hanya ngerti menggunakan perangkat tersebut. Namun, tidak demikian Ruby Alamsyah. Barang bukti digital merupakan santapan lezatnya. Sepak terjangnya di dunia forensik digital pun layak diacungi jempol. Banyak kasus besar yang ditangani Mabes Polri maupun Polda Jakarta melibatkan jasanya sebagai seorang Digital Forensic Analyst (DFA).

Seperti apakah seluk-beluk dunia forensik digital yang digeluti Ruby Alamsyah dan tokoh-tokoh lainnya? Apa urgensi profesi ini dalam penuntasan kasus-kasus kriminal?

Langka Pesaing
â€œTugas saya sebagai DFA adalah menganalisis barang bukti digital yang ditemukan polisi,â€• terang Ruby. â€œUntuk kasus video yang baru-baru ini terjadi, tugas saya tentu melacak siapa yang menjadi penyebar pertama, berikut barang bukti lainnya yang memiliki memori. Kalau menganalisis keaslian foto/video bukan wewenang saya,â€• imbuh pria kelahiran Jakarta, 23 November 1974 ini.

Peranan seorang ahli forensik digital di era teknologi seperti saat ini, boleh jadi terbilang penting. Ilmu forensik memiliki andil yang besar dalam menganalisis barang bukti digital. Turunan ilmu IT Securityini memang bertugas menganalisis barang bukti digital secara ilmiah demi menemukan bukti suatu tindak kejahatan. Barang bukti tersebut tentu harus dapat dipertanggungjawabkan dengan baik di mata hukum.

Menurut Ruby, barang bukti digital yang bisa dianalisis tidak melulu notebook, tapi juga personalcomputer (PC), handphone, PDA, MP3 player, dan sebagainya. Menurut pria yang menjadi satu-satunya warga Indonesia anggota High Technology Crime Investigation Association/HTCIA ini, semuayang memiliki memori, baik itu memori internal maupun eksternal dapat dianalisis.

Untuk masuk ke organisasi yang mayoritas anggotanya terdiri dari para polisi itu tidaklah mudah. Sebagian besar wajib memiliki track record baik dalam melewati kasus-kasus besar dan mengungkap jejak digital menjadi sebuah barang bukti yang kuat di pengadilan. Untuk menangani kasus besar pun harus ada referensi dari polisi atau penegak hukum di negara setempat, sejumlah sertifikasi yang dimiliki, sertaresume. Seluruh persyaratan tadi lalu dibawa ke semacam rapat komite. Nah, di sinilah baru ditetapkan apakah seseorang bisa menjadi member HTCIA atau tidak. Faktor inilah yang lantas memunculkan anggapan bahwa menjadi anggota HTCIA tidaklah mudah. Â

Ruby sendiri sudah mengantongi 4 sertifikasi di bidang forensik digital, yaitu GCIH (GIAC Certified Incident Handler) dari SANS Institute, USA; GCFA (GIAC Certified Forensic Analyst) dari SANS Institute, USA; CHFI (Computer Hacking Forensic Analyst) dari EC-Council, USA; ENCE (Encase Certified Examiner), dari Guidance Software; dan ACE (Accessdata Certified Examiner), dari AccessData.

Untuk mendapatkan sertifikasi-sertifikasi tersebut, sebagian besar harus melalui training resmi terlebih dahulu. Setiap training pun berbeda jangka waktunya. â€œRata-rata 1 sampai dengan 2 minggu. Itu hanya training saja,

untuk ujiannya ada yang mengambil langsung setelah training, ada juga yang menunggu beberapa waktu untuk belajar lebih detail lagi baru mengambil ujiannya,â€• jelas Ruby.
â€œAda satu sertifikasi DF yang setelah lulus ujian tertulis, akan diberikan ujian praktik (dengan barang bukti digital Asli) dan diberi waktu selama 60 hari untuk menyelesaikannya,â€• ungkapnya. Sertifikasi di sini sebenarnya adalah sebagai penunjang/pendukung keahlian seseorang. Pada akhirnya pendidikan formal dan pengalaman jualah yang akan menentukan porsi keahlian seseorang. Artinya untuk menjadi seorang DFA, seseorang minimal harus memiliki latar belakang pendidikan TI.
Diakui Ruby, dirinya tertarik dengan forensik digital karena pesaingnya masih sedikit. Orang yang seperti Ruby memang masih sedikit. Pasalnya banyak orang TI yang enggan bersentuhan dengan dunia kepolisian, politisi, maupun hukum di Indonesia. Klien seorang DFA pun tidak sebarangan. â€œKlien saya sejak tahun 2006, sebagian besar adalah penegak hukum (Polri dan Kejaksaan. red). Mulai tahun 2009 sudah mulai banyak klien korporasi maupun klien individu. Saya sudah pernah menjadi saksi ahli di persidangan kasus perdata dan pidana (di pengadilan negeri.red), serta pengadilan di Badan Arbitrase Nasional,â€• urainya. Ruby juga bercerita, dirinya bahkan sempat mendapat bayaran 5 ribu dolar untuk tiga puluh menit.Â

Melacak Penyebar Pertama Video
Khusus untuk kasus tersebarnya video syur yang lalu, tugas seorang DFA adalah melacak pelaku penyebar pertama yang meng-upload video. Yang pertama-tama dilakukan adalah melakukan analisis/riset secara mendalam dan menyeluruh guna mengetahui siapa individu yang lebih dahulu memiliki file tersebut. Langkah yang ditempuh misalnya melakukan pelacakan awal mula penyebaran (dari yang melakukan penyebaran pada hari H), lalu meruut dan melacak siapa yang memiliki data tersebut paling awal.

Dalam hal ini sangat dimungkinkan untuk juga melacak IP address bila tidak diketahui secara pasti siapa individu tersebut. Untuk memudahkan pekerjaan, seorang DFA diperbolehkan melakukan kerjasama dengan ISP terkait yang memiliki log pelanggannya. ID-SIRTII pun bisa dimintai bantuan guna mendapatkan data lebih lanjut. Dari sini akan bisa menjadi peringatan bagi kita untuk tidak sebarang mengunggah foto/video ke dunia maya.

Seperti prajurit yang sedang bertempur, seorang DFA juga menggunakan "senjata" dalam melakukan pelacakan. Ruby menjabarkan aneka software yang digunakan biasanya tergantung dari kebutuhan setiap kasus. Namun, bila sudah mendapatkan barang bukti digital secara fisik, baru dilakukan proses forensik digital secara detail. Namun sebelum itu, tekniknya bisa menggunakan e-discovery.

Bagi yang masih awam, e-discovery merupakan teknik pencarian data elektronik, di mana data elektronik tersebut ditempatkan/berada, serta bagaimana mengamankan dan menyitanya untuk dapat dijadikan barang bukti pada sebuah kasus. E-discovery dapat dilakukan pada komputer tertentu, atau pun pada jaringan tertentu. Pada bidang forensik digital, e-discovery merupakan proses investigasi yang dilakukan terhadap harddisk pada komputer tertentu. Barang bukti tersebut selanjutnya mengalami proses kloning (forensic imaging).

Perangkat yang digunakan untuk melakukan computer forensic dan mobile phone forensic pun berbeda. â€œUntuk computer forensic, saya menggunakan Encase v6.15, FTK 3, Sleuthkit-Autospy, Helix, dd, Forensic Duplicator (Tbleau-TD1), Forensic Write Blocker, dan lain-lain. Sementara untuk [melakukan] mobile phone forensic, menggunakan Cellbrite, XRY/XACT, Paraben Device Seizure, Bitpim, dan lain-lain,â€• jelasnya.

Adakah kesulitan yang dialami? Pasti ada. Biasanya Ruby mengalami kendala ketika menjumpai aneka file yang tersembunyi (steganography) dan terenkripsi. â€œSeperti layaknya criminal non-cyber, biasanya sepintar-pintarnya penjahat pasti akan meninggalkan jejak. Tinggal sepintar-pintarnya tim penyidik untuk mendapatkan jejak apa yang tertinggal,â€• jelas pria yang biasa mengisi waktu senggangnya dengan membaca buku dan menonton film ini. Ada tools dan teknik-teknik tertentu untuk menyiasati masalah tersebut. Misalnya untuk menghadapi steganography, penyelidik bisa menggunakan software â€œSteg-detectâ€• guna mendapatkan file

tersembunyi tersebut.

Demikian halnya untuk pelaku tindak kejahatan cyber yang menggunakan jaringan wireless. Pelacakan dapat dilakukan dengan mencari log serta data-data lain, misalnya berupa CCTV tempat jaringan itu berada. Lalu, bagaimana jika yang dilacak adalah individu yang sedang menggunakanmobile phone? â€œTentu saja pelacakan bisa dilakukan secara remote/mobile,â€• tegas Ruby.
Ruby juga menjelaskan proses penyelidikan setiap tindak kejahatan cyber sudah pasti membutuhkanbandwidth. Namun menurutnya, bandwidth bukanlah hal utama, pun tidak perlu menggunakan bandwidth besar-besar, karena bukan untuk melakukan offensive attack. Bandwidth hanya dibutuhkan untuk koneksi internet saja, tidak lebih.Â

Prosedur Forensik Digital
Seperti juga pekerjaan profesional lainnya, seorang DFA harus mematuhi peraturan keanggotaan yang sudah ditetapkan.â€œJika saya melanggar, saya bisa dikeluarkan dari keanggotaan (HTCIA, red),â€• beber Ruby.
Istimewanya, seorang DFA dapat memberikan masukan kepada penegak hukum tentang barang bukti digital apa saja yang mungkin terkait dalam sebuah kasus, selain merekomendasikan proses penyitaan, melakukan proses cloning barang bukti digital, melakukan proses analisis, membuat laporan, sampai menjadi saksi ahli di persidangan bila dibutuhkan.

Dalam menjalankan tugasnya, ada 4 (empat) langkah yang menjadi prosedur operasional standar (standard operating prochedure/SOP) seorang DFA.

1. Mengkloning barang bukti digital yang sudah ada di polisi. Kloning di sini menggunakan metodologi khusus byte by byte copy cloning.
2. Menganalisis barang bukti dari barang duplikasi. Jadi bukan barang bukti asli yang diteliti karena bisa rusak. Jika barang bukti asli rusak, kasus bisa gagal. Barang bukti berubah satu byte saja bisa rusak dan dianggap tidak valid.
3. Melakukan proses recovery dan analisis lebih lanjut.
4. Melakukan reporting. Ruby menambahkan bahwa analisis harus dilakukan pada barang bukti duplikasi, bukan yang asli. Hal ini untuk menghindari kehilangan/perubahan/kerusakan data pada barang bukti asli.

Menariknya, bidang forensik digital ini mengawinkan dua disiplin ilmu, yakni *ilmu komputer* dan *ilmu hukum*. Untuk Indonesia, pasar seperti ini masih sangat luas. â€œIT di Indonesia ke depannya bersinggungan dengan dunia hukum, which is every day akan selalu ada potential market,â€• tegas Ruby. Mulai dari penegak hukun, kuasa hukum, sampai korporasi maupun individu menjadi pasar potensial (potential market) dari forensik digital (digital forensic). Tidak dapat dipungkiri pula bahwa tindak kriminal setiap hari semakin meningkat. Apalagi melihat ketergantungan individu terhadap perangkat teknologi yang semakin meningkat pula. Dapat dipastikan pula bahwa kemungkinan besar di setiap kasus kriminal mana pun, akan terdapat barang bukti digital yang dapat dianalisis dengan forensik digital.

Mewakili seorang DFA, Ruby mengaku masih memiliki impian yang ingin dicapai. Nantinya, ia berharap Indonesia dapat segera memiliki aturan/guideline tentang proses penanganan barang bukti digital (yang tepat dan baik bagi penegak hukum pada khususnya). UU ITE serta RUU Tipiti dapat menjadi batu pijakan untuk dapat segera merealisasikan aturan tersebut. Pada akhirnya semua kasus yang berhubungan dengan barang bukti digital dapat ditangani dengan tepat dengan integritas yang terjaga secara utuh.

Melacak Wajah
Ilmu forensik tidak melulu harus terkait dengan notebook/harddisk. Apalagi jika barang bukti tindak kejahatan berhubungan dengan foto/video. Biasanya yang digunakan adalah forensik bidang kedokteran. Misalnya saja kasus bom bunuh diri teroris atau tersebarnya video biru yang lalu. Untuk mengungkap kasus seperti itu,

digunakanlah suatu teknik bernama superimposed. Di sinilah kemampuan seorang ahli seperti drg. Peter Sahelangi, DFM (Senior Superintendent (Ret)Forensic Odontologist) diperlukan.
â€œSuperimposisi Cranio FacialÂ adalah suatus sistem pemeriksaan untuk menentukan jati diri seseorang dengan membandingkan foto korban/rekaman video semasa hidupnya (ante mortem) dengan tengkorak/ jenazah korban yang ditemukan kemudian (post mortem),â€• jelas mantan Kepala Rumah Sakit (RS) Polri tahun 1976-2008 ini.
Prinsip kerjanya yaitu dengan cara membandingkan titik anatomis dalam wajah/tengkorak yang tidak bisa berubah/diubah kemudian ditumpangtindihkan/ superimposed (dengan teknik-teknik tertentu dan alat-alat tertentu yang disebut skull mounting & orientation device (SMOD). Teknik ini dapat dilakukan pada jenazah dan tentu saja orang yang masih hidup.

Yang bisa melakukan teknik ini pun tidak sebarangan orang. Untuk melakukan hal ini, diperlukan seorang yang setidaknya memiliki pengetahuan anatomi tubuh secara baik, misalnya dokter/dokter gigi. Ilmu forensik yang dimiliki Peter diakuinya didalami dengan cara kursus. Itu pun gampang-gampang susah. Menurutnya, orang tersebut juga harus mengenal pribadi si expert atau berkawan dengan mereka, baru mereka mau terbuka menularkan ilmunya.
Peter juga bercerita mengenai kasus yang heboh sekarang, yang dulu juga pernah terjadi di Malaysia (saat video seks seorang pejabat dengan artis-artis Malaysia tersebar). Alat yang digunakan pun sama, yakni menggunakan SMOD.
Untuk melakukan analisis terhadap foto/gambar, tidak ada prosedur khusus seperti seorang DFA (yang harus melalui empat tahap). â€œYang penting ada surat permintaan dari penyidik, [baru akan] kami laksanakan,â€• jelas pria kelahiran 60 tahun silam ini. Selain SMOD, masih ada beberapa perangkat lain yang digunakan, seperti video dan komputer dengan program Adobe Photoshop.

Lamanya waktu analisis pun berbeda-beda. â€œTergantung sulit tidaknya kasus dan kualitas foto pembanding, posisi, dan lain-lain. [Lamanya proses] bisa [berlangsung] beberapa jam, bisa juga beberapa hari,â€• terang Peter. Sebagai seorang expert, Peter hanya menjawab cocok atau tidaknya titik-titik anatomisnya. â€œSoal asli atau tidaknya bukan wewenang kami,â€• tegas pria yang kini menjadi dosen Bagian Forensik & Medikolegal Fakultas Kedokteran UNHAS Makassar serta dosen terbang di beberapa fakultas kedokteran gigi beberapa perguruan tinggi di Indonesia.

Hampir setiap pekerjaan memiliki kendala masing-masing. Bagi Peter, kendala yang kerap ia hadapi misalnya jika korban tidak pernah difoto seumur hidupnya (untuk korban yang sudah meninggal). â€œAda kasus pembunuhan di Ambon yang tengkoraknya dikirim pada kami, tapi korban tidak pernah mempunyai foto/tidak pernah difoto,â€• jelas Peter. â€œKualitas foto yang sangat jelek, tengkorak yang ditemukan sudah hancur tidak berbentuk kepala manusia lagi. Posisi korban yang tidak optimal, misalkan menyamping, tertutup orang lain juga menjadi kendala,â€œ tukasnya.

Menantang Kejelian Mata
Video heboh yang tersebar beberapa waktu lalu, sempat memicu kecurigaan publik terhadap si pelaku yang ada di video tersebut.
Sebagai awam, pasti ada di antara kita yang langsung menuding, â€œ Ya, benar itu si A, atau itu memang si B. Gosip baru, nih.â€•Padahal kenyataannya, belum tentu itu si A atau si B. Bisa saja si C. Oleh karena itu, dibutuhkan teknik khusus untuk membuktikannya.

â€œMenganalisa video bisa menggunakan setting slow motion, contohnya menggunakan Windows Media Player (WMP). Dengan slow motionÂ ini, akan keliatan asli atau tidaknya gerakan tersebut,â€• ujar Abimanyu Wachjoewidajat, pria yang kerap dimintai keterangan terkait analisa foto/ video.

Gambar yang ada di video tersebut kemudian di-compare dengan foto lainnya yang dicari di internet.

â€œUkurannya pun harus sama, tidak boleh berbeda,â€• tukas pria yang akrab di sapa Abah ini. Tugas selanjutnya adalah mencocokkan posisi. Untuk analisis dengan teknik slow motion ini, tidak melulu menggunakan WMP, dapat juga menggunakan Winamp atau Windows Media Classic yang ada di komputer kita. â€œApa saja bisa, asal media tersebut bisa [melakukan teknik] slow motion agar ketika gambar diperbesar tidak pecah,â€• imbuh Abimanyu. Â

Sementara untuk menganalisis foto, bisa menggunakan teknik morphing. â€œDengan demikian posisi mata, hidung, bibir akan kelihatan kemiripannnya,â€• jelas Abimanyu. â€œMenggunakan teknik morphingini juga tidak boleh memaksa, karena kalau memaksa hasil gambarnya tidak valid,â€• tegas pria yang pernah menjabat sebagai Data Center Manajer PT. Excelcomindo ini. Proporsinya pun harus sama. Misal naik 5 persen dan ke kanan 5 persen. Itu harus sama.

Menganalisis foto/video, dijelaskan Abimanyu harus dalam suasana tenang. Jadi tidak bisa dilakukan secara mobile karena akan susah. Kendala lainnya adalah dalam menganalisis kemiripan. Contohnya gambar. Selain itu adalah mencari gambar-gambar lainnya yang mirip melalui internet. Abimanyu juga menyatakan bahwa dalam menganalisis foto/gambar, kita tidak bisa melakukannya secara asal-asalan. (di re-post dari berbagai sumber)

All is about imagination - Endang Kurniawan
Sumber : https://endangkurniawan.com/article-menelusuri-jejak-forensik-dari-beberapa-kasus.html