

UTS Forensik Digital
Alvaro Austin - 2106752180

Forensik digital merupakan bidang studi dan juga praktik yang berhubungan erat dengan pengumpulan, analisis, serta interpretasi bukti digital dalam rangka melakukan penyelidikan tindakan kriminal yang melibatkan teknologi komputer, perangkat digital, dan jaringan. Untuk mempelajari praktek nyata dari pekerjaan seorang forensik digital, terdapat beberapa studi kasus yang dapat menggambarkan tantangan investigasi. Melalui studi kasus yang dilakukan secara kelompok (Nitroba, M57 Jean, M57 Patent, Lonewolf cases), saya mempelajari beberapa hal penting terutama dalam sisi *cybercrime*. Melalui studi kasus tersebut, kita diberikan sumber data digital yang lengkap yang melibatkan tindak kejahatan digital seperti *harassing*, *data leak*, *blackmail*, *pornography*, dll.

Kolaborasi dan komunikasi dalam tim merupakan hal utama yang sangat penting dalam melakukan forensik digital. Berdasarkan pengalaman saya kemarin, komunikasi dan kolaborasi tidak hanya membuat pengerjaan menjadi lebih cepat namun juga memberikan saya kesempatan untuk bertukar pikiran dengan sesama anggota kelompok. Proses bertukar pikiran ini membantu saya memikirkan kemungkinan lain yang terjadi pada dunia nyata. Proses ini tentunya penting karena sebagai seorang forensik digital, tidak boleh bertindak banyak berdasarkan “asumsi” yang kita buat.

Selanjutnya, kasus *cybercrime* seringkali memiliki kompleksitas yang tinggi. Kompleksitas ini melibatkan berbagai macam aplikasi dan pelaku untuk membuktikan suatu kasus *cybercrime* tersebut. Setiap kasus biasanya membutuhkan aplikasi yang berbeda-beda seperti Forensics Toolkit, Autopsy, dsb. Pemilihan aplikasi ini biasanya membutuhkan pengetahuan yang cukup dalam rangka mengoperasikan aplikasi tersebut dengan baik. Tanpa pengetahuan yang cukup, biasanya proses investigasi akan tertunda sehingga menyebabkan hasil yang kurang maksimal.

Hal yang saya pelajari dan sangat penting pada forensik digital adalah proses forensik digital dalam mencari bukti tindakan kejahatan digital dengan hukum dan undang-undang. Undang-undang memberikan kerangka kerja yang jelas tentang bagaimana bukti digital dapat dikumpulkan, disajikan, dan diterima di pengadilan. Tanpa dasar hukum yang tepat, bukti digital mungkin saja tidak sah atau dapat diperdebatkan di pengadilan. Selain itu, kita juga harus menentukan pelanggaran undang-undang yang tepat terhadap tindakan kejahatan digital yang

tepat. Apabila kita salah dalam menentukan pelanggaran undang-undang, bukti-bukti digital yang kita lampirkan mungkin saja tidak relevan. Oleh karena itu, penting sekali sebagai seorang yang melakukan forensik digital untuk mengerti hukum yang terkait terhadap kasus yang mereka tangani. Akan tetapi, hal yang sebaliknya juga berlaku, apabila seorang pengacara berusaha menangani kasus kejahatan digital, mereka juga perlu mencari bukti-bukti digital yang berkaitan. Jadi, kegiatan forensik digital dan hukum (undang-undang) sangat berkaitan erat satu dengan yang lain.

Akan tetapi pada saat melakukan studi kasus tersebut, tantangan tentu saja muncul untuk setiap kasus yang diinvestigasi. Salah satu tantangan tersebut adalah pemilihan sumber data yang membutuhkan memori komputer yang besar. Tidak hanya itu, biasanya pada dunia nyata, data yang tersedia cenderung sedikit karena banyak pelaku tindakan kejahatan digital berusaha untuk menghapus jejak digital mereka. Hal ini dapat membuat kegiatan pencarian bahan bukti menjadi semakin sulit.

Tantangan diatas bisa diatasi dengan beberapa cara. Untuk mengatasi tantangan memori komputer yang besar, kita dapat menambahkan memori yang dialokasikan untuk menganalisa bahan bukti analisis. Setelah investigasi selesai, kita juga dapat menghapus bukti-bukti investigasi setelah memberikan hasil investigasi diberikan kepada pihak yang terkait. Dengan begitu, pengalokasian memori tidak akan menjadi masalah yang besar. Selanjutnya untuk mengatasi tantangan data yang diselidiki berjumlah sedikit, biasanya hal ini terjadi karena pelaku berusaha menghapus jejak digital mereka. Hal ini dapat kita atasi dengan menggunakan aplikasi-aplikasi untuk melakukan hal seperti *file carving* (mengembalikan file yang sudah dihapus), kerja sama dengan pihak ketiga seperti IP Provider, dll.

Selanjutnya, pemilihan bukti yang relevan juga menjadi tantangan yang terjadi dalam setiap investigasi yang dilakukan. Terkadang bukti yang dipilih kurang cukup, bisa terjadi karena adanya *human error* maupun kekurangan data yang dapat diinvestigasi. Oleh karena itu, untuk menghadapi tantangan tersebut, kita dapat berkomunikasi dengan tim. Komunikasi ini dapat berupa pendapat maupun meminta bantuan melalui sumber data lain. Dengan begitu, kita dapat mendapatkan hasil investigasi yang lebih baik.

Proses melakukan investigasi forensik digital sangat krusial untuk hasilnya. Setiap kelalaian dalam langkah-langkah atau mengubah urutan mereka dapat mengarah pada hasil yang tidak lengkap, dan oleh karena itu interpretasi dan kesimpulan yang salah. Oleh karena itu,

metodologi dan pendekatan yang diadopsi dalam forensik digital perlu terus ditingkatkan dan disederhanakan. Kabar baiknya, masa depan forensik digital kemungkinan akan melihat perbaikan di beberapa area, didasarkan pada kemajuan sejak **Digital Forensic Research Workshop (DFRWS)** pada 2007.

Salah satu area spesifik yang bisa ditingkatkan adalah penanganan *digital evidence bags* (DEBs). DEBs mempertahankan informasi provenansial mengenai bukti digital. Namun, metodologi DEB saat ini tidak merujuk informasi zona waktu dan representasi timestamp saat berurusan dengan beberapa sumber bukti digital dari berbagai zona waktu. Mampu mengabstraksi representasi bukti digital dan korelasi waktu dari beberapa sumber adalah area kunci untuk penelitian dan pengembangan di masa depan.

Aspek lain yang penting adalah standarisasi dan peningkatan alat akuisisi forensik. Akuisisi adalah bagian penting dari proses forensik digital, dan penelitian telah menghasilkan beberapa teknik dan alat akuisisi baru. Namun, proses ini sering mengarah pada penyidik mendapatkan lebih banyak data daripada yang diperlukan, yang dapat menghasilkan waktu yang hilang dalam investigasi. Kemajuan di masa depan mungkin melibatkan penyempurnaan alat ini agar lebih efisien dan tepat.

Terakhir, ada kebutuhan untuk peningkatan kerangka kerja analisis. Analisis memerlukan kerangka kerja yang mengatur proses investigasi forensik dan memungkinkan inklusi alat baru untuk memahami dan menginterpretasikan data secara holistik. Ini akan mendukung model abstraksi yang mempertahankan integritas data sambil juga memungkinkan peningkatan kemampuan analisis.

Sehingga berdasarkan hasil yang diperoleh pada DFRWS 2007, masa depan forensik digital kemungkinan akan melibatkan penyempurnaan proses investigasi, evolusi metode penanganan bukti, pengembangan alat akuisisi yang lebih efisien, dan penciptaan kerangka kerja analisis yang lebih maju. Kemajuan area-area ini akan membantu proses forensik digital dalam segi waktu maupun tenaga kerja sehingga proses investigasi menjadi semakin cepat.