Digital Forensic Pada *Cyber Crime* Dan Bagaimana Universitas Udayana Ikut Berperan Di Dalamnya

I Putu Agus Eka Pratama, S.T, M.T,[1]
[1]Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Udayana
Email: eka_pratama@unud.ac.id

Highlight

***Cyber Crime* dan *Digital Forensic* menjadi dua hal penting di jaman teknologi informasi saat ini. Indonesia belum memiliki banyak SDM handal di bidang ini, namun kebutuhan akan SDM ini cukup besar. Hal ini menjadi peluang bagi Universitas Udayana untuk dapat ikut berperan di dalamnya. Untuk itulah, maka tulisan ini mencoba mengetengahkan sekilas tentang *Digital Forensic* dan *Cyber Crime*, serta bagaimana upaya yang dapat dilakukan oleh Universitas Udayana untuk dapat ikut berperan di dalamnya.**

Kata kunci : *Digital Forensic, Cyber Crime,* Universitas Udayana

Gambar Topik (Sesuai Dengan Artikel ditampilkan di Website)

Sumber : http://www.uokufa.edu.iq/it/images/Digital%20forensics.jpg

Pendahuluan

Pada jaman teknologi informasi saat ini, *Cyber Crime* dan *Digital Forensic* adalah dua hal yang saling berhubungan. *Cyber Crime* atau disebut juga dengan *Computer Crime*, merupakan segala tindakan yang dilakukan secara langsung maupun tidak langsung melalui komputer dan jaringan komputer (termasuk juga melalui internet) yang melanggar etika, hukum, dan wewenang, terkait dengan pemrosesan data dan pengiriman data [1]. *Digital Forensic* merupakan salah satu dari 8 buah cabang ilmu forensik (*Forensic Science*), sebagai bentuk respon dari

adanya *Cyber Crime*, yang didukung oleh penyediaan bukti – bukti yang sah (*Legitimate Evidence*) [2]. Ketujuh buah cabang lainnya dari ilmu forensik selain *Digital Forensic* adalah : *Chemistry Forensic*, *Biology Forensic*, *Ballistic Forensic*, *Document Forensic*, *Toxicology Forensic*, *Narcotic Forensic*, dan *Medicine Forensic*. Cabang ilmu *Digital Forensic* dibagi lagi menjadi 10 buah sub bidang ilmu dengan karakteristik dan peran masing - masing, yang meliputi : *Computer Forensic*, *Cyber Forensic*, *Triage Forensic*, *Malware Forensic*, *Anti Forensic*, *Memory Forensic*, *Audio Forensic*, *Image Forensic*, *Mobile Forensic*, dan *Video Forensic* [3]. Keterkaitan antara *Cyber Crime* dan *Digital Forensic* bukan saja untuk pemenuhan bukti otentik di dalam persidangan dan hukum, tapi juga melihat dari sisi pengguna dan jaringan komputer. Hal ini mengingat bahwa jaringan komputer secara sistem terdiri atas sejumlah *layer*, *hardware*, dan *software*, sehingga keamanan pada jaringan komputer juga harus melihat 3 aspek utama (*system*, *policy*, *user*) dan 3 poin utama (*confidentiality*, *integrity*, *availability*) untuk mewujudkan kenyamanan dan kepercayaan pengguna [4]. Di Indonesia, SDM bidang *Digital Forensic* tidak sebanyak kasus *Cyber Crime* yang terjadi. Saat ini, Mabes Polri adalah salah satu lembaga pemerintah yang menyediakan dukungan SDM untuk penanganan *Cyber Crime* menggunakan ilmu dan SDM *Digital Forensic*. Di sinilah perlunya peran penting dari institusi pendidikan di Indonesia (dalam hal ini perguruan tinggi) untuk ikut berperan mencetak SDM handal di bidang ini, termasuk juga Universitas Udayana.

Uraian Isi

Untuk saat ini, ketersediaan sarana pendukung (lab) dan SDM di bidang forensik serta keikut sertaan di dalam membantu kasus yang ada, telah dilakukan oleh Universitas Udayana melalui UPT Lab *Forensic Science* dan *Crimonology*, salah satunya pada kasus sidang pembunuhan Mirna [5]. Sedangkan mata kuliah mengenai *Digital Forensic*, salah satunya telah diajarkan di Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Udayana, melalui mata kuliah IT *Forensic* (kode : TI025336). Untuk dapat menjadikan Universitas Udayana dapat turut berperan di dalam penyelesaian kasus *Cyber Crime* menggunakan keilmuan dan SDM di bidang Digital Forensic, terdapat 3 langkah yang dapat dilakukan. Pertama, perlu adanya penyediaan lab riset dan pendukung lainnya (komputer, internet, intranet, buku, akses jurnal, software). CAINE adalah salah satu distribusi (distro) sistem operasi Linux yang direkomendasikan untuk *Digital Forensic*, khususnya *Computer Forensic* untuk kasus *Cyber Crime*, dengan sejumlah tool di dalamnya [6]. Kedua, berbekal ketersediaan mata kuliah IT *Forensic* dan ketersediaan lab riset, maka memudahkan dosen dan mahasiswa/i untuk mempraktekkan teori yang ada. Untuk lebih lanjut, dapat dilakukan studi kasus nyata di lapangan, misalkan bekerja sama dengan Polda Bali, yang diterapkan ke dalam bentuk tugas kuliah, penelitian, Tugas Akhir, publikasi, project, dan lainnya. Ketiga, perlu mengundang narasumber yang berkompeten di bidang *Digital Forensic*, baik lokal maupun internasional, misalnya Muhammad Nuh Al Azhar, salah satu ahli *Digital Forensic* Indonesia dari POLRI sekaligus ketua Asosiasi Forensik Digital Indonesia (AFDI). Rekan – rekan riset di IDSIRTII, bagian dari Kemkominfo RI untuk keamanan di dunia cyber, juga dapat

menjadi rekomendasi untuk narasumber lainnya (terutama *Malware Forensic* dan *Mobile Forensic*). Di luar ketiga langkah tersebut, di internal Universitas Udayana, hendaknya juga dapat melakukan penelitian bersama lintas keilmuan (jurusan/program studi/fakultas), mengingat bahwa Digital Forensic (sebagaimana halnya forensik di dunia nyata), melibatkan sejumlah bidang ilmu. Sebagai contoh ide, kerja sama Fakultas Hukum, Fakultas Teknik, dan Fakultas MIPA untuk studi kasus *cyber crime* menggunakan *Digital Forensic*, bekerja sama dengan Polda Bali, dalam bentuk project dan penelitian. Manfaat yang diperoleh oleh Universitas Udayana dengan keikut sertaannya di dalam penanganan *Cyber Crime* menggunakan *Digital Forensic*, secara umum dapat berupa peningkatan prestasi dan prestise institusi di tingkat lokal, nasional, bahkan internasional. Selain itu, juga mampu meningkatkan jumlah penelitian, publikasi, kerja sama dengan pihak lain, peningkatan kualitas SDM dan kualitas alumni, penyerapan lulusan ke dunia kerja, hingga dalam bentuk finansial melalui kerja sama *project* (swasta dan pemerintah). Kebutuhan akan SDM di bidang *Digital Forensic* akan terus bertambah, seiring dengan makin pesatnya perkembangan dan pemanfaatan teknologi informasi di semua lini kehidupan. Ini merupakan peluang yang harus dimanfaatkan dengan sebaik – baiknya.

Kesimpulan

SDM di bidang *Digital Forensic* makin banyak diperlukan di tengah maraknya kasus *Cyber Crime*. Universitas Udayana dapat turut serta di dalam penanganan kasus *Cyber Crime* menggunakan keilmuan *Digital Forensic* ini, melalui penyediaan sarana pendukung, kerja sama dengan berbagai pihak dan studi kasus langsung di lapangan, serta mengundang narasumber. Sehingga diharapkan Universitas Udayana dapat melahirkan SDM handal di bidang ini, baik dari kalangan dosen, mahasiswa/i, dan alumni. Institusi dan civitas akademisi, sama – sama memperoleh sejumlah manfaat dari hal ini.

Referensi

1. I. P. A. E. Pratama. *Komputer dan Masyarakat* (Bab 9 Cyber Crime). Informatika. Bandung. 2014.
2. M. N. Al Azhar. The Essential Of Digital Forensic. Code Bali International Cyber Security Conference 2016. Bali, Indonesia. 2016.
3. M. N. Al Azhar. *Digital Forensic : Practical Guidelines for Computer Investigation*. Salemba Infotek. Jakarta. 2012.
4. I. P. A. E. Pratama. *Handbook Jaringan Komputer* (Bab 10 Keamanan Pada Jaringan Komputer). Informatika. Bandung. 2014.
5. Rimadi, Luqman. Liputan 6 News. 2016. (http://news.liputan6.com/read/2599451/ahli-forensik-udayana-ungkap-proses -sianida-larut-di-kopi-mirna (diakses 5 Februari 2017).
6. CAINE Computer Forensic Linux Live Distro. (http://www.caine-live.net/ (diakses 5 Februari 2017).