

ABSTRAK

Cybercrime (Kejahatan Dunia Maya) adalah kejahatan yang dilakukan oleh seseorang atau sekelompok orang atau korporasi dengan cara menggunakan atau dengan sasaran komputer atau sistem komputer atau jaringan komputer yang mempunyai karakteristik berbeda dengan kejahatan tradisional, permasalahan yang dapat dirumuskan diantaranya kejahatan yang merupakan *cybercrime* menurut Undang-undang Nomor 11 Tahun 2008, dan Pembuktian *Cybercrime* dalam proses Penegakkan Hukum di Indonesia, serta hambatan-hambatan dan solusi dalam pembuktian *Cybercrime* dalam proses penegakan hukum di Indonesia.

Penggunaan metode *Yuridis Sosiologis* dilakukan untuk meneliti data sekunder atau bahan pustaka berkaitan dengan Tinjauan Yuridis Pembuktian *Cybercrime*, kemudian pada Spesifikasi penelitian ini bersifat *deskriptif analisis*, karena diharapkan mampu memberi gambaran secara rinci, sistematis, dan menyeluruh terhadap obyek yang akan diteliti terkait dengan Pembuktian *Cybercrime* Dalam Proses Penegakan Hukum di Indonesia, serta Sumber data yang dipergunakan dalam penelitian ini yaitu Data Primer sebagai data utama lapangan yang relevan dengan pemecahan masalah dan pembahasan yang didapat dari sumber utama penelitian, kemudian Data sekunder yang didapat dari data kepustakaan yang digunakan dalam penelitian.

Hasil penelitian dapat disimpulkan sebagai berikut; Jenis Kejahatan Yang Merupakan *Cybercrime* Menurut Undang-Undang Nomor 11 Tahun 2008 diantaranya Kejahatan yang Menggunakan Teknologi Informasi Sebagai Fasilitas: Pembajakan, Pornografi, Pemalsuan/ Pencurian Kartu Kredit, Penipuan Lewat Email (Fraud), Email Spam, Perjudian Online, Pencurian Account Internet, Terorisme, Isu Sara, Situs Yang Menyesatkan, dan Kejahatan yang Menjadikan Sistem Teknologi Informasi Sebagai Sasaran: Pencurian Data Pribadi, Pembobolan/Pembajakan Situs, Pembuktian *Cybercrime* dalam proses penegakkan Hukum di Indonesia dapat dimulai dengan melakukan investigasi kasus dengan cara mencari alamat ip address web dan mencari bukti elektronik. Karena ip address web adalah bukti pertama yang kuat didalam pengungkapan kasus cyber, sesuai pasal 5 Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi elektronik, Hambatan dan Solusi Pembuktian *Cybercrime* dalam Proses penegakkan Hukum di Indonesia diantaranya pada Perangkat hukum yang belum memadai, Kemampuan penyidik masih sangat minim, Alat Bukti Sangat Rapuh, Fasilitas komputer forensik Kurang memadai, Sedangkan solusi yang harus dilakukan untuk mengatasi hambatan dalam pembuktian *cybercrime* Perlu dibuat undang-undang yang khusus mengatur *Cybercrime*, diperlukan penyidik yang cukup berpengalaman menguasai teknis penyidikan dan pengetahuan di bidang komputer dan profil hacker, serta Fasilitas *forensic computing* yang dapat melayani tiga hal penting yaitu *evidence collection, forensic analysis, expert witness*.

Kata Kunci : *Cybercrime* Kejahatan tanpa batas.

ABSTRACT

Cybercrime (Cyber Crime) is a crime committed by a person or group of persons or corporations by means of use or with the target computer or computer system or computer network that has different characteristics with traditional crime, problems that can be formulated such crime is cybercrime according to Law law No. 11 of 2008, and in the process of evidence Cybercrime law enforcement in Indonesia, as well as obstacles and solutions in the proof of cybercrime in the process of law enforcement in Indonesia.

Use of the method Juridical Sociological conducted to examine secondary data or library materials related to Review Judicial Evidence Cybercrime, then the specification of this research is descriptive analysis, because it is expected to give a detailed description, systematic and thorough review of the object to be examined associated with Proof Cybercrime in the process of Law Enforcement in Indonesia, as well as the source of data used in this study are primary data as the main data field relevant to problem solving and discussion obtained from the primary source research, and secondary data obtained from literature data used in the study.

It can be concluded as follows; Type of Crime That Is Cybercrime According to Law No. 11 of 2008 of which Crime Using Information Technology As Facilities: Piracy, pornography, forgery / Credit Card Theft, Fraud by Email (Fraud), Email Spam, Online Gambling, Theft Internet Accounts, Terrorism Issues Sara, Trip the misleading and Crime Makes Information Technology Systems Targeting: Theft of Personal Data, Piercing / PembajakanSitus, evidence Cybercrime in the process of enforcement of law in Indonesia can begin to investigate the case by seeking the address ip address web and search for evidence electronic. Because web ip address is the first strong evidence in the case of cyber disclosure, in accordance with Article 5 of Law No. 11 Year 2008 on Information and Electronic transactions, Obstacles and Solutions Evidence Cybercrime in the process of the rule of law in Indonesia, including the legal instruments are not sufficient, Ability investigators are still very minimal, Evidence Very Fragile, amenities computer forensics less adequate, while solutions must be done to overcome obstacles in proving cybercrime is a need for legislation that specifically regulate cybercrime requires investigators who are experienced enough to master the technical investigation and knowledge in the field of computer and profiles hackers, as well as amenities forensic computing which can serve three important things namely evidence collection, forensic analysis, expertwitness.

Keywords: Crime Cybercrime indefinitely.