



Utilization of Digital Forensics in Proving the Crime of Disseminating Indecent Videos Through Facebook Social Media in the Legal Area of West Kalimantan Police

Pemanfaatan Digital Forensik Dalam Pembuktian Tindak Pidana Penyebaran Video Asusila Melalui Media Sosial Facebook Di Wilayah Hukum Polda Kalbar

M Qahar Awaka ¹⁾

¹⁾ Universitas Tanjungpura Pontianak

Email: ¹⁾ Muhammad.qahar.awaka@hukum.untan.ac.id

No HP/ WhatsApp Author:

ARTICLE HISTORY

Received [15 September 2023]

Revised [19 Oktober 2023]

Accepted [29 Oktober 2023]

KEYWORDS

digital forensics, evidence, social media

This is an open access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license



ABSTRAK

Penelitian yang berjudul: "Pemanfaatan Digital Forensik Dalam Pembuktian Tindak Pidana Penyebaran Video Asusila Melalui Media Sosial Facebook Di Wilayah Hukum Polda KALBAR" bertujuan Untuk mengetahui serta memaparkan pelaksanaan informasi dan hasil penelitian di kota Pontianak serta untuk mengetahui dan menganalisis pemanfaatan digital forensik dalam pembuktian tindak pidana penyebaran video asusila melalui media sosial facebook di wilayah hukum polda KALBAR. Penelitian ini dilakukan dengan menggunakan metode pendekatan yuridis sosiologis yaitu mengkaji dan mengolah data hasil penelitian lapangan dengan bertitik tolak pada aspek hukum secara normatif dengan didukung dokumen-dokumen yang berkaitan dengan permasalahan baik berupa peraturan maupun kasus-kasus yang terkait dengan pokok permasalahan Berdasarkan penelitian dan analisis data dapat diperoleh informasi bahwa pelaksanaan Digital Forensik terkait dengan tindak pidana penyebaran video asusila melalui media sosial Facebook adalah suatu proses penyelidikan dan analisis terhadap bukti digital yang terkait dengan tindakan kejahatan tersebut. Dalam kasus ini, bukti digital yang menjadi fokus adalah video asusila yang menyebar melalui platform media sosial Facebook. Di bahas dalam beberapa topik penting yakni; 1. Peranan Digital Forensik Terkait Tindak Pidana Penyebaran Video Asusila Melalui Media Sosial Facebook, 2. Faktor Apa Yang Menjadi Penghambat Dalam Pembuktian Melalui Digital Forensik Terkait Tindak Pidana Penyebaran Video Asusila Melalui Media Sosial Facebook, 3. Upaya Apa Yang Telah Dilakukan Dalam Optimalisasi Pembuktian Digital Forensik Terkait Tindak Pidana Penyebaran Video Asusila Melalui Facebook. Kesimpulan yang dapat di sampaikan pada penelitian ini adalah Penerapan digital forensik melibatkan beberapa tahapan penting, di antaranya identifikasi bukti digital, penyimpanan bukti digital, analisis bukti digital, dan presentasi hasil temuan. Digital forensik memiliki peran krusial dalam melakukan pembuktian dalam kasus-kasus hukum. Di Indonesia, sistem pembuktian mensyaratkan minimal dua alat bukti yang sah dan keyakinan dari Hakim untuk menentukan kesalahan terdakwa. Dalam kasus tindak pidana cyber crime, alat bukti elektronik harus memenuhi persyaratan baik secara formil maupun materiil agar dianggap sah dan dapat diterima di persidangan. Oleh karena itu, penerapan digital forensik dalam penyidikan tindak pidana cyber crime, khususnya penyebaran video asusila, memiliki peran penting dalam menemukan alat bukti dan barang bukti elektronik yang relevan untuk proses peradilan.

ABSTRACT

The research entitled: "Utilization of Digital Forensics in Proving the Crime of Disseminating Indecent Videos Through Facebook Social Media in the KALBAR Police Legal Area" aims to find out and describe the implementation of information and research results in Pontianak city and to find out and analyze the utilization of digital forensics in proving the crime of spreading indecent videos through Facebook social media in the KALBAR police jurisdiction. This research was conducted using a sociological juridical approach method, namely examining and processing data from field research by starting from normative legal aspects supported by documents related to the problem in the form of regulations and cases related to the subject matter Based on research and data analysis, information can be obtained that the implementation of Digital Forensics related to the criminal act of spreading immoral videos through Facebook social media is a process of investigating and analyzing digital evidence related to the crime. In this case, the digital evidence that is the focus is an immoral video that spreads through the Facebook social media platform. Discussed in several important topics, namely; 1. The Role of Digital Forensics Related to the Crime of Dissemination of Indecent Video Through Facebook Social Media, 2. What Factors Become Obstacles in Proof Through Digital Forensics Related to the Crime of Dissemination of Indecent Video Through Facebook Social Media, 3. What Efforts Have Been Made in Optimizing Digital Forensic Evidence Related to the Crime of Immoral Video Dissemination Through Facebook. The conclusion that can be conveyed in this research is that the application of digital forensics involves several important stages, including the identification of digital evidence, storage of digital evidence, analysis of digital evidence, and presentation of findings. Digital forensics has a crucial role in proving legal cases. In Indonesia, the evidentiary system requires a minimum of two valid pieces of evidence and the conviction of the Judge to determine the guilt of the defendant. In the case of cyber crime, electronic evidence must meet

both formal and material requirements to be considered valid and admissible in court. Therefore, the application of digital forensics in the investigation of cyber crime, especially the distribution of immoral videos, has an important role in finding relevant electronic evidence and evidence for the judicial process.

PENDAHULUAN

Perkembangan teknologi adalah sebuah hal yang tidak bisa dihindari dampaknya bagi kehidupan manusia karena beriringan dengan kemajuan ilmu pengetahuan. Secara esensial, teknologi diciptakan untuk mempermudah berbagai aktivitas manusia dalam kehidupan sehari-hari. Salah satu bidang yang mengalami perkembangan akibat kemajuan teknologi adalah komunikasi, dan salah satu bentuknya adalah gadget. Gadget merupakan perangkat elektronik dengan fungsi khusus, seperti telepon pintar, yang pada dasarnya dibuat untuk memberikan kemudahan dan kenyamanan hidup bagi manusia. Gadget hadir dengan berbagai aplikasi yang menyajikan berbagai macam media, seperti berita, jejaring sosial, hobi, dan hiburan.

Sejak tahun 2022, data menunjukkan bahwa penggunaan gadget di Indonesia telah mengalami peningkatan yang signifikan. Pada tahun tersebut, jumlah pengguna gadget mencapai 65,2 juta jiwa, yang kemudian melonjak tajam menjadi 92 juta jiwa pada tahun 2022. Selain itu, pengguna telepon seluler di Indonesia secara keseluruhan mencapai 371,4 juta pengguna, yang setara dengan 142 persen dari total populasi sekitar 262 juta jiwa. Hal ini berarti rata-rata setiap penduduk Indonesia memiliki 1,4 telepon seluler, dengan beberapa orang bahkan menggunakan 2 hingga 3 kartu telepon seluler. Populasi kaum urban di Indonesia mencakup sekitar 55 persen dari total populasi. Selain itu, jumlah pengguna internet di Indonesia juga mencapai angka yang signifikan, yaitu sekitar 132,7 juta, dengan tingkat penetrasi sekitar 51 persen dari seluruh populasi. Penggunaan gadget telah menjadi suatu kebutuhan utama bagi manusia karena dipengaruhi oleh berbagai faktor, salah satunya adalah meningkatnya jumlah produksi gadget yang beredar di Indonesia. Kondisi ini mengakibatkan semakin banyak masyarakat Indonesia yang akhirnya memiliki kesempatan dan kemampuan untuk membeli serta menggunakan gadget. Penggunaan gadget oleh beberapa individu yang cenderung menyimpang terlihat dari perilaku mereka yang mengakses konten berunsur pornografi. Data terkait total situs porno saat ini mencapai antara 28 hingga 30 juta, bahkan dalam periode satu tahun, Kementerian Komunikasi dan Informatika telah melakukan pemblokiran terhadap sebanyak 773 ribu situs pada tahun 2022. Saat ini, dunia maya (virtual world) dan World Wide Web telah diisi dengan jumlah yang sangat besar konten pornografi atau yang berkaitan dengan masalah seksual. Diperkirakan bahwa 40 persen dari berbagai situs di World Wide Web menyediakan bahan-bahan berunsur asusila, dan topik ini menjadi salah satu yang paling menarik perhatian di internet. Asusila juga menjadi salah satu topik yang paling banyak dicari di internet. Lebih dari 25 persen pengguna internet dilaporkan mengunjungi lebih dari 60 ribu situs berunsur pornografi setiap bulannya, dan jumlah orang yang mengakses situs berunsur pornografi mencapai sekitar 30 juta orang setiap harinya. Meningkatnya jumlah situs atau konten yang berkaitan dengan video asusila sejalan dengan peningkatan penggunaan gadget sebagai perangkat elektronik. Fenomena ini menyebabkan jumlah kejahatan dengan bukti elektronik menjadi semakin banyak yang harus dihadapi oleh investigator dalam penanganan kasus kejahatan. Perkembangan kejahatan sangat terpengaruh oleh kemajuan teknologi, yang dapat menghasilkan dua dampak yang berbeda tergantung pada bagaimana teknologi tersebut dimanfaatkan. Dampak tersebut dapat bersifat positif atau negatif. Salah satu aspek positif dari perkembangan teknologi adalah pemanfaatannya dalam mengungkap kejahatan.

Melakukan investigasi terhadap kejahatan untuk mengungkapkan kebenaran, pemanfaatan teknologi komputer yang bersifat positif sangat penting. Aplikasi ilmu pengetahuan dan teknologi komputer menjadi kunci dalam memeriksa dan menganalisis setiap barang bukti elektronik dan digital. Tujuan dari analisis ini adalah untuk melihat keterkaitan antara bukti digital yang satu dengan yang lain, sehingga kejahatan dapat terungkap dengan jelas dalam proses pengungkapannya. Dengan demikian, pelaku kejahatan dapat dipertanggungjawabkan atas perbuatannya. Salah satu bentuk pengaplikasian teknologi komputer tersebut adalah melalui ilmu pengetahuan tentang Digital forensik. Digital forensik merupakan teknik analisis dan investigasi yang memiliki tahapan-tahapan dalam prosesnya. Teknik ini digunakan untuk menganalisis dan menginterpretasi media data digital yang tersimpan dengan tujuan utama yaitu untuk mencari pembuktian yang relevan dengan kasus yang sedang ditangani.

Menurut Muhammad Nuh Al-Azhar dalam bukunya digital forensik Panduan dapat dibagi menjadi beberapa spesialisasi, seperti komputer forensik, mobile forensik, audio forensik, video forensik, dan image forensik. Salah satu contoh penggunaan Digital forensik adalah dalam penanganan kasus konten Asusila yang belum lama ini terjadi. Sebuah kasus video asusila ditangani oleh Subdit Siber Ditreskrimsus Polda Kalimantan Barat. Berdasarkan praobservasi penulis, kasus ini melibatkan video yang memperlihatkan adegan bermuatan asusila antara pelapor dan pelaku saat melakukan hubungan



badan. Video tersebut kemudian tersebar di media sosial, sehingga Subdit Siber Ditreskrimsus Polda Kalimantan Barat melakukan penyelidikan terhadap kasus ini.

Tabel 1 Data Kasus Penyebaran Video Asusila Melalui Media Sosial

No	Tahun	Jumlah	Keterangan
1	2021	7 kasus	Tahap 2
2	2022	4 Kasus	Tahap 2

Sumber : Subdit Siber Ditreskrimsus Polda Kalbar

LANDASAN TEORI

Pengertian Penegakan Hukum

Penegakan hukum adalah suatu usaha untuk menanggulangi kejahatan secara rasional, memenuhi rasa keadilan dan berdaya guna. Dalam rangka menanggulangi kejahatan terhadap berbagai sarana sebagai reaksi yang dapat diberikan kepada pelaku kejahatan, berupa sarana pidana maupun non hukum pidana, yang dapat diintegrasikan satu dengan yang lainnya. Apabila sarana pidana dipanggil untuk menanggulangi kejahatan, berarti akan dilaksanakan politik hukum pidana, yakni mengadakan pemilihan untuk mencapai hasil perundang-undangan pidana yang sesuai dengan keadaan dan situasi pada suatu waktu dan untuk masa-masa yang akan datang.

Penegakan hukum dapat dilakukan dengan berupa penindakan hukum. Abdul Kadir Muhammad menjelaskan bahwa penindakan hukum dapat dilakukan dengan urutan sebagai berikut:

- Teguran peringatan supaya menghentikan pelanggaran dan jangan berbuat lagi (percobaan);
- Pembebanan kewajiban tertentu (ganti kerugian, denda);
- Penyisihan atau pengucilan (pencabutan hak-hak tertentu);
- Pengenaan sanksi badan (pidana penjara, pidana mati).

Pengertian Tindak Pidana

Tindak pidana adalah perbuatan yang oleh aturan hukum dilarang dan diancam dengan pidana, di mana pengertian perbuatan di sini selain perbuatan yang bersifat aktif yaitu melakukan sesuatu yang sebenarnya dilarang oleh undang-undang dan perbuatan yang bersifat pasif yaitu tidak berbuat sesuatu yang sebenarnya diharuskan oleh hukum. Menurut Barda Nawawi Arief, tindak pidana adalah perbuatan melakukan atau tidak melakukan sesuatu yang oleh peraturan perundang-undangan dinyatakan sebagai perbuatan yang dilarang dan diancam dengan pidana. Tindak pidana dibagi menjadi dua bagian yaitu :

- Tindak pidana materil (materiel delict)

Tindak pidana yang dimaksudkan dalam suatu ketentuan hukum pidana (straf) dalam hal ini sirumuskan sebagai perbuatan yang menyebabkan suatu akibat tertentu, tanpa merumuskan wujud dari perbuatan itu

- Tindak pidana formal (formeel delict).

Apabila perbuatan tindak pidana yang dimaksudkan dirumuskan sebagai wujud perbuatan tanpa menyebutkan akibat yang disebabkan oleh perbuatan itu, inilah yang disebut tindak pidana formal (formeel delict).

Pengertian Tindak Pidana Di Bidang Informasi dan Transaksi Elektronik

Pengertian Tindak Pidana

Pidana berasal dari kata straf (Belanda), yang ada kalanya disebut dengan istilah hukuman. Istilah pidana lebih tepat dari istilah hukuman, karena hukum sudah lazim merupakan terjemahan dari Recht. Menurut Moelyatno, hukum pidana adalah bagian dari pada keseluruhan hukum yang berlaku di suatu negara, yang mengadakan dasar-dasar dan aturan-aturan untuk :

- Menentukan perbuatan-perbuatan mana yang tidak boleh, yang dilarang, dengan disertai ancaman atau sanksi yang berupa pidana tertentu bagi barangsiapa melanggar larangan tersebut.
- Menentukan kapan dan dalam hal-hal apa kepada mereka yang telah melanggar larangan-larangan itu dapat dikenai atau dijatuhi pidana sebagaimana yang telah diancamkan.
- Menentukan dengan cara bagaimana penggunaan pidana itu dapat dilaksanakan apabila ada orang yang disangka telah melanggar larangan tersebut.

Strafbaarfeit dalam bahasa Belanda berasal dari dua unsur pembentuk kata, yaitu strafbaar dan feit. Perkataan feit dalam bahasa Belanda diartikan "sebagian dari kenyataan", sedangkan strafbaar

berarti “dapat dihukum”, sehingga secara harafiah perkataan strafbaarfeit berarti “sebagian dari kenyataan yang dapat dihukum” yang sudah tentu tidak tepat. Bahwa di sini yang dapat dihukum adalah manusia pribadi bukan kenyataan, perbuatan atau tindakan. Sedangkan menurut J.E Jonkers, peristiwa pidana adalah perbuatan yang melawan hukum (wederrechtelijk) yang berhubungan dengan kesengajaan atau kesalahan yang dilakukan oleh orang yang dapat dipertanggungjawabkan.

Mengenai definisi dari tindak pidana ada 2 (dua) pandangan yang berbeda dari para sarjana yakni pandangan dualisme dan pandangan monisme. Pertama, Pandangan dualisme adalah pandangan yang memisahkan antara perbuatan dan orang yang melakukan. Menurut Moeljatno, perbuatan pidana adalah “perbuatan yang dilarang oleh suatu aturan hukum, larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barang siapa yang melanggar larangan tersebut. Dapat juga dikatakan bahwa perbuatan pidana adalah perbuatan yang dilarang hukum dan diancam pidana, asal saja dalam hal itu diingat bahwa larangan ditujukan pada perbuatannya (yaitu kejadian atau keadaan yang ditimbulkan oleh kelakuan orang, sedang ancaman pidananya ditujukan pada orang yang menimbulkan kejahatan).

Pengertian Informasi Elektronik dan Transaksi Elektronik

Pengertian Informasi Elektronik

Informasi bukanlah hanya sebagai suatu obyek ataupun output saja, yang lazim diartikan dalam bahasa Indonesia sebagai suatu keterangan ataupun berita, melainkan juga harus melihat kepada aspek pemrosesannya. Dengan kata lain validitas informasi sangat ditentukan oleh sejauh mana validitas pemrosesannya. Dengan kata lain, informasi bersumber dari data yang telah diproses. Sedangkan yang dimaksud dengan informasi elektronik dapat berupa catatan elektronik, data atau dokumen elektronik, surat-surat elektronik, ataupun tanda tangan elektronik.

Informasi elektronik merupakan salah satu hal yang diatur secara substansial dalam UU ITE selain transaksi elektronik. Perkembangan pemanfaatan informasi elektronik dewasa ini, sudah memberikan kenyamanan dan kemanfaatannya. Sebagai contoh, penggunaan e-mail sangat memudahkan setiap orang bisa berkomunikasi melalui pengiriman berita secara cepat, dan dapat melintasi wilayah baik lokal, regional, dan bahkan hingga internasional. Pemanfaatan penyebaran informasi elektronik ini, telah memberikan manfaat dengan menjamurnya usaha kecil dan menengah yang bergerak bidang penjualan jasa seperti warung-warung internet (Warnet). Di samping itu, penyebaran arus informasi elektronis ini, juga dimanfaatkan untuk ajang silaturahmi untuk mencari teman-teman baru yang dikenal dengan facebook, yang sedang digandrungi oleh kaum remaja.

Pemanfaatan informasi elektronik ini, juga dimanfaatkan oleh kalangan pemerintah, seperti lembaga-lembaga pemerintah baik sipil maupun TNI/Polri, Komisi Pemilihan Umum Indonesia, untuk secara otomatis memanfaatkan informasi elektronik untuk kepentingan pengawasan dan pengendalian fungsi pemerintahan, dewasa ini, untuk mencegah terjadinya praktek-praktek kolusi, korupsi, dan nepotisme, beberapa instansi pemerintahan sudah menyelenggarakan suatu system nobody-contact, seperti instansi Kementerian Hukum dan HAM, dalam hal pengangkatan pejabat notaris dan Pejabat Pembuat Akta Tanah (PPAT), dan pejabat calon pendaftar hanya mengirimkan berkas permohonan melalui loket-loket dan pengumuman keberatan diterima atau tidaknya diumumkan melalui mass media cetak atau melalui e-mail sehingga informasi itu tidak dapat diakses.

Pengertian Transaksi Elektronik

Dalam ketentuan umum Pasal 1 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik disebutkan bahwa Transaksi Elektronik adalah : “perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer dan atau media elektronik lainnya”. Transaksi elektronik dirumuskan definisinya dari terminologi E-commerce (Electronic Commerce) atau mengarah pada perniagaan atau perdagangan, namun dalam Undang-undang Informasi dan Transaksi tidak mendefinisikan E-commerce secara jelas. E-commerce dapat didefinisikan sebagai segala bentuk transaksi perdagangan/ perniagaan barang atau jasa (trade of goods and servic) dengan menggunakan media elektronik. Electronic Commerce adalah kemampuan untuk membentuk transaksi bisnis yang meliputi pertukaran barang dan jasa diantara dua pelaku bisnis dengan menggunakan peralatan dan teknologi elektronika. Perbuatan hukum penyelenggaraan transaksi elektronik dapat dilakukan dalam lingkup publik ataupun privat. Para pihak yang melakukan transaksi elektronis wajib beritikad baik dalam melakukan interaksi dan/atau pertukaran informasi elektronik dan atau dokumen elektronik selama transaksi berlangsung. Penyelenggaraan transaksi elektronis ini diatur dengan peraturan pemerintah.

Transaksi elektronik diatur dalam Pasal 17 Undang-undang Nomor 11 Tahun 2008 yang berbunyi sebagai berikut :

(1) penyelenggaraan transaksi elektronik dapat dilakukan dalam lingkup publik dan privat;



- (2) Para pihak yang melakukan transaksi elektronik sebagaimana dimaksud pada butir (i) wajib beritikad baik dalam melakukan interaksi dan/atau pertukaran informasi elektronik dan atau dokumen elektronik selama transaksi berlangsung”;
- (3) Ketentuan lebih lanjut mengenai penyelenggaraan transaksi elektronik sebagaimana dimaksud pada ayat (i) diatur dengan Peraturan Pemerintah.

Pembuktian Tindak Pidana Di Bidang Informasi dan Transaksi Elektronik Pembuktian Dalam Hukum Acara Pidana Di Indonesia

Pembuktian merupakan masalah yang memegang peranan sidang pengadilan melalui pembuktian ditentukan nasib terdakwa. Apabila hasil pembuktian dengan alat-alat bukti yang ditentukan undang-undang tidak cukup membuktikan kesalahan yang didakwakan kepada terdakwa, maka terdakwa dibebaskan dari hukuman. Sebaliknya, kalau kesalahan terdakwa dapat dibuktikan dengan alat bukti yang disebut dalam Pasal 184 KUHP, terdakwa dinyatakan bersalah kepadanya akan dijatuhkan oleh karena itu, hakim harus berhati-hati, cermat, dan matang menilai dan mempertimbangkan nilai pembuktian meneliti sampai dimana batas minimum kekuatan pembuktian atau Bewijs Kracht dari setiap alat bukti yang disebut dalam Pasal 184 KUHP.

Pembuktian bersalah tidaknya seseorang terdakwa haruslah melalui pemeriksaan di depan sidang pengadilan. Dalam hal pembuktian ini, hakim perlu memperhatikan kepentingan masyarakat dan kepentingan terdakwa. Kepentingan masyarakat berarti, bahwa seseorang yang telah melanggar ketentuan pidana (KUHP) atau undang-undang pidana lainnya, harus mendapat hukuman yang setimpal yang kesalahannya. Sedangkan kepentingan terdakwa, berarti bahwa terdakwa harus diperlakukan secara adil sedemikian rupa sehingga tidak ada seseorang yang tidak bersalah mendapat hukuman, atau kalau memang ia bersalah jangan sampai mendapat hukuman yang terlalu berat, tetapi hukuman itu harus seimbang dengan kesalahannya.

Begitu pula dalam cara mempergunakan dan menilai kekuatan pembuktian yang melekat pada setiap alat bukti, dilakukan dalam batas-batas yang dibenarkan undang-undang, agar dalam mewujudkan kebenaran yang hendak dijatuhkan, majelis hakim terhindar dari pengorbanan kebenaran yang harus dibenarkan. jangan sampai kebenaranyang diwujudkan dalam putusan berdasar hasil perolehan dan penjabaran yang keluar dari garis yang dibenarkan sistem pembuktian. tidak berbau dan diwarnai oleh perasaan dan pendapat subjektif hakim.

Ditinjau dari segi hukum acara pidana sebagaimana yang ditentukan dalam KUHP, telah diatur beberapa pedoman dan penggarisan :

- a. Penuntut umum bertindak sebagai aparat yang diberi wewenang untuk mengajukan segala daya upaya membuktikan kesalahan yang didakwakan kepada terdakwa.
- b. Sebaliknya terdakwa ataupun penasihat hukum mempunyai hak untuk melumpuhkan pembuktian yang diajukan penuntut umum, sesuai dengan cara-cara yang dibenarkan undang-undang, berupa “sangkalan” atau bantahan yang beralasan, dengan saksi yang meringankan atau saksi a decharge maupun dengan “alibi”.
- c. Pembuktian juga bisa berarti suatu penegasan bahwa ketentuan tindak pidana lain yang harus dijatuhkan kepada terdakwa. Maksudnya, surat dakwaan penuntut umum bersifat alternatif, dan dari hasil kenyataan pembuktian yang diperoleh dalam persidangan pengadilan, kesalahan yang terbukti adalah tidak sesuai dengan kenyataan pembuktian. Dalam hal seperti ini, arti dan fungsi pembuktian merupakan penegasan tentang tindak pidana yang dilakukan terdakwa, serta sekaligus membebaskan dirinya dari dakwaan yang tidak terbukti dan menghukumnya berdasar dakwaan tindak pidana yang telah terbukti.

Keterangan Ahli

Keterangan seorang ahli disebut sebagai alat bukti pada urutan yang kedua setelah keterangan saksi oleh Pasal 183 KUHP. Didalam Pasal 186 KUHP menyatakan bahwa keterangan seorang ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan. Tidak diberikan penjelasan yang khusus mengenai apa yang dimaksud dengan keterangan ahli menurut KUHP, dan menurut Andi Hamzah dapat merupakan kesenjangan pula.

Dalam terjemahan yang dikemukakan oleh Andi Hamzah, seseorang dapat memberikan keterangan sebagai ahli jika ia mempunyai pengetahuan, keahlian, pengalaman, latihan, atau pendidikan khusus yang memadai untuk memenuhi syarat sebagai seorang ahli tentang hal yang berkaitan dengan keterangannya. KUHP membedakan keterangan ahli di persidangan sebagai alat bukti “keterangan ahli” (Pasal 186 KUHP) dan keterangan seorang ahli secara tertulis di luar sidang pengadilan sebagai alat bukti “surat” (Pasal 187 butir c KUHP). Contohnya ialah visum et repertum yang dibuat oleh seorang dokter. Seorang ahli dapat memberikan keterangan mengenai tandatangan dan tulisan sebagai alat bukti dalam hal terjadi pemalsuan tandatangan dan tulisan tangan. Hal ini termuat dalam Surat

Edaran Jaksa Agung RI kepada jajaran kejaksaan di seluruh Indonesia No.SE-003/J.A/2/1984 yang merupakan aturan pelaksanaan dari Pasal 184 ayat (1) huruf c jo. Pasal 187 KUHAP. Tetapi menurut Yahya Harahap :Keterangan Ahli hanya sebatas mengenai keterangan ahli tentang tandatangan dan tulisan. Jika tandatangan atau tulisan hendak dijadikan alat bukti, untuk menentukan autentikasi tanda tangan dan tulisan tersebut, ahli yang dimintai keterangannya untuk itu menurut SE Jaksa Agung untuk tindak pidana umum dan tindak pidana khusus, keterangan ahli autentikasi diberikan oleh LABKRIM MABAK.

Pada pemeriksaan penyidikan demi untuk kepentingan peradilan, penyidik berwenang mengajukan permintaan keterangan dari seorang ahli. Apabila keterangan ahli bersifat 'diminta', ahli tersebut membuat laporan sesuai dengan yang dikehendaki penyidik. Laporan tersebut menurut penjelasan Pasal 186 KUHAP dibuat dengan mengingat sumpah di waktu ia menerima jabatan atau pekerjaan. Oleh penjelasan Pasal 186, laporan seperti itu bernilai sebagai alat bukti keterangan ahli, yang diberi nama "alat bukti keterangan ahli berbentuk laporan". Apabila hal itu tidak diberikan pada waktu pemeriksaan oleh penyidik atau penuntut umum maka pada pemeriksaan di sidang, seorang ahli diminta untuk memberikan keterangan dan dicatat dalam berita acara pemeriksaan. Keterangan tersebut diberikan setelah ia mengucapkan sumpah atau janji di hadapan hakim.

Surat

Selain Pasal 184 KUHAP yang menyebutkan alat-alat bukti secara limitatif, didalam Pasal 187 diuraikan tentang alat bukti surat yang terdiri dari empat butir. Asser-Anema memberikan pengertian, surat ialah segala sesuatu yang mengandung tanda-tanda baca yang dapat dimengerti, dimaksud untuk mengeluarkan isi pikiran. Sedangkan menurut A. Pitlo adalah pembawa tanda tangan bacaan yang berarti, yang menerjemahkan suatu pikiran. Tidak termasuk kata surat, adalah foto dan peta, sebab benda ini tidak memuat tanda bacaan.

Surat sebagaimana tersebut dalam Pasal 184 ayat (1) huruf c, dibuat atas sumpah jabatan atau dikuatkan dengan sumpah adalah :

- 1) Berita acara dan surat lain dalam bentuk resmi yang dibuat oleh pejabat umum yang berwenang atau yang dibuat dihadapannya, yang memuat keterangan tentang kejadian atau keadaan yang didengar, dilihat atau yang dialaminya sendiri, disertai dengan alasan yang jelas dan tegas tentang keterangannya itu.
- 2) surat yang dibuat menurut ketentuan peraturan perundang-undangan atau surat yang dibuat oleh pejabat mengenai hal yang termasuk dalam tata laksana yang menjadi tanggung jawabnya dan yang diperuntukkan bagi pembuktian sesuatu hal atau sesuatu keadaan.
- 3) surat keterangan dari seorang ahli yang memuat pendapat berdasarkan keahliannya mengenai sesuatu hal atau sesuatu keadaan yang diminta secara resmi daripadanya.
- 4) surat lain yang hanya dapat berlaku jika ada hubungannya dengan isi dari alat pembuktian yang lain.

Petunjuk

Petunjuk merupakan alat bukti keempat yang disebutkan dalam Pasal 184 KUHAP. Dalam Pasal 188 ayat (1) disebutkan pengertian petunjuk, yaitu perbuatan, kejadian atau keadaan, yang karena persesuaiannya, baik antara yang satu dengan yang lain, maupun dengan tindak pidana itu sendiri, menandakan bahwa telah terjadi satu tindak pidana dan siapa pelakunya. Yahya Harahap mendefenisikan petunjuk dengan menambah beberapa kata yakni petunjuk adalah suatu "isyarat" yang dapat ditarik dari suatu perbuatan, kejadian atau keadaan dimana isyarat tadi mempunyai persesuaian antara yang satu dengan yang lain maupun isyarat tadi mempunyai persesuaian dengan tindak pidana itu sendiri, dan dari isyarat yang bersesuaian tersebut "melahirkan" atau mewujudkan suatu petunjuk yang membentuk kenyataan terjadinya suatu tindak pidana dan terdakwa pelakunya. Menurut Pasal 188 ayat (2) KUHAP dalam hal cara memperoleh alat bukti petunjuk, hanya dapat diperoleh dari :

- 1) Keterangan saksi;
- 2) Surat; dan
- 3) Keterangan terdakwa.

Keterangan Terdakwa

Pengertian keterangan terdakwa tercantum dalam Pasal 189 ayat (1) KUHAP yang berbunyi : "keterangan terdakwa ialah apa yang terdakwa nyatakan di sidang tentang perbuatan yang ia lakukan atau yang ia ketahui atau alami sendiri". Keterangan terdakwa yang diberikan di luar sidang dapat digunakan untuk membantu menemukan bukti di sidang, asalkan keterangan itu didukung oleh suatu alat bukti yang sah sepanjang mengenai hal yang didakwakan kepadanya. Keterangan terdakwa hanya dapat digunakan terhadap dirinya sendiri. Keterangan terdakwa saja tidak cukup untuk membuktikan bahwa ia bersalah melakukan perbuatan yang didakwakan kepadanya, melainkan harus disertai dengan alat bukti



yang lain. Terhadap bunyi Pasal 189 ayat (2), Yahya Harahap mengatakan keterangan yang dapat diklasifikasikan sebagai keterangan terdakwa yang diberikan di luar sidang adalah :

- 1) keterangan yang diberikannya dalam pemeriksaan penyidikan;
- 2) dan keterangan itu dicatat dalam berita acara penyidikan;
- 3) serta berita acara penyidikan itu ditandatangani oleh pejabat penyidik dan terdakwa.

Pembuktian Perkara Pidana Menurut Undang-undang Diluar KUHAP

KUHAP tidak mengatur mengenai alat bukti data elektronik, namun beberapa peraturan Perundang-undangan menyebutkan bahwa data elektronik dapat dijadikan sebagai alat bukti yang sah. Berikut akan diuraikan beberapa peraturan Perundang-undangan yang mengatur tentang pembuktian dengan data elektronik sebagai alat bukti.

Pembuktian Tindak Pidana Di Bidang Informasi dan Transaksi Elektronik Menurut UU No 11 Tahun 2008

Dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 5 ayat 1 dan 2 mendeskripsikan bahwa Dokumen Elektronik dan Informasi adalah merupakan alat bukti yang sah. Selain itu dalam Pasal 44 Undang-undang yang sama mengatakan : “Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut :

- 1) alat bukti sebagaimana dimaksud dalam ketentuan Perundangan; dan
- 2) alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).”

Pasal 1 angka 1 UU No 11 Tahun 2008 “Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.”

Pada Pasal 5 Undang-Undang Nomor 11 Tahun 2008 dijelaskan bahwa :

- (1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
- (2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
- (3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.
- (4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk: a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta.

Informasi adalah bersumber dari data yang telah diproses. Informasi elektronik dapat berupa catatan elektronik, data atau dokumen elektronik, surat elektronik ataupun tanda tangan elektronik. Suatu data/informasi yang telah diolah oleh sistem informasi secara elektronik tersebut akan tersimpan didalam suatu media tertentu secara elektronik, yang dinamakan dokumen elektronik. Sistem penyimpanan data/atau informasi elektronik yang berbasis komputer dinamakan Databases dan data yang dikomunikasikan melalui media telekomunikasi dinamakan Data Messages. Data messages inilah yang menjadi landasan utama terbentuknya suatu kontrak elektronik, baik dalam hubungannya dengan kesepakatan mengenai persyaratan-persyaratan dan ketentuan-ketentuan kontrak (terms and conditions) ataupun yang berkaitan dengan substansi kontrak itu sendiri.

Testamentary Evidence

Testamentary Evidence juga dikenal dengan istilah Hearsay Evidence dimana keterangan ahli dan saksi maupun expert witness yaitu keterangan dari seorang ahli dapat diberikan selama persidangan, berdasarkan pengalaman dan pengamatan individu. Peranan dari keterangan ahli sesuai dengan peraturan perundang-undangan kita yaitu UU No 8 Tahun 1981 KUHAP, bahwa keterangan ahli dinilai sebagai alat bukti yang mempunyai kekuatan pembuktian jika keterangan yang diberikan tentang sesuatu hal berdasarkan keahlian khusus dalam bidang yang dimilikinya dan yang berupa keterangan “menurut pengetauannya” secara murni. .

Circumstantial Evidence

Circumstantial Evidence adalah merupakan bukti terperinci yang diperoleh berdasarkan ucapan atau pengamatan dari kejadian yang sebenarnya yang mendorong untuk mendukung suatu kesimpulan, tetapi bukan untuk membuktikannya. Circumstantial evidence atau derived evidence ini merupakan kombinasi dari real evidence dan hearsay evidence.

Di dalam UU No. 11 Tahun 2008 diatur mengenai pembuktian, yang terdapat pada BAB X tentang Penyidikan, khususnya pada Pasal 43 ayat 5e dan 5h. Pasal 43 Ayat 5e UU No 11 Tahun 2008 "melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana berdasarkan Undang-Undang ini" Pihak yang dimaksud berhak untuk melakukan penyidikan atau pemeriksaan sebagaimana yang tertera dalam Pasal 43 ayat (1) adalah Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik. Pasal 43 Ayat 5h UU No 11 Tahun 2008 "meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana berdasarkan Undang-Undang ini" Pembuktian sebagai salah satu faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannya pun bisa demikian kompleks dan rumit.

METODE PENELITIAN

Jenis Penelitian

Penelitian ini dilakukan dengan menggunakan metode pendekatan yuridis sosilogis yaitu mengkaji dan mengolah data hasil penelitian lapangan dengan bertitik tolak pada aspek hukum secara normatif dengan didukung dokumen- dokumen yang berkaitan dengan permasalahan baik berupa peraturan maupun kasus-kasus yang terkait dengan pokok permasalahan.

Penelitian ini didasarkan pada penelitian kepustakaan dan penelitian lapangan dengan penjelasan sebagai berikut :

- a. Penelitian Kepustakaan, yaitu penelitian yang dilakukan dengan cara mengumpulkan data dari berbagai pustaka yang berhubungan dengan masalah yang akan diteliti.
- b. Penelitian Lapangan, yaitu merupakan pelengkap yang diperoleh dari beberapa responden yang terlibat dalam kegiatan UU ITE daerah Kota KALBAR serta aparatur pemerintah daerah dan Kepolisian yang terlibat.

HASIL DAN PEMBAHASAN

Peranan Digital Forensik Terkait Tindak Pidana Penyebaran Video Asusila Melalui Media Sosial Facebook

Pembuktian perkara pidana bertujuan untuk mencari kebenaran materiil, yaitu kebenaran sejati atau yang sesungguhnya. Sedangkan dalam hukum acara perdata, pembuktian perkara perdata bertujuan untuk mencari kebenaran formil, artinya hakim tidak boleh melampaui batas-batas yang diajukan oleh para pihak yang berperkara. Jadi, ketika hakim mencari kebenaran formal dalam perkara perdata, cukup membuktikan dengan "preponderance of evidence," sedangkan hakim dalam perkara pidana harus meyakini bahwa peristiwa yang diajukan terbukti "beyond reasonable doubt" . pembuktian dalam terminologi, menurut kamus Besar Bahasa Indonesia, adalah proses atau cara untuk membuktikan suatu pernyataan atau fakta, serta merupakan upaya untuk menentukan kebenaran atau kebenaran dari pihak terdakwa dalam sidang pengadilan. Dalam konteks ini, pembuktian menjadi unsur penting dalam hukum acara pidana karena digunakan untuk menentukan apakah seseorang terdakwa bersalah atau tidak di dalam persidangan. Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) telah menetapkan alat bukti yang sah menurut undang-undang, yang terdiri dari (1). Keterangan Saksi, (2). Keterangan Ahli, (3). Surat, (4). Petunjuk, (5). Keterangan Terdakwa.

Menurut Yahya Harahap, dalam Buku Pembahasan, Permasalahan, dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali, Pasal 184 ayat (1) KUHAP secara jelas telah menentukan alat bukti yang sah menurut undang-undang. Diluar jenis-jenis alat bukti tersebut, penggunaan bukti tidak dibenarkan untuk membuktikan kesalahan terdakwa. Para pihak yang terlibat dalam sidang, seperti Ketua sidang, penuntut umum, terdakwa, atau penasihat hukum, terikat dan hanya diperbolehkan menggunakan alat-alat bukti yang telah ditentukan oleh Pasal 184 ayat (1) KUHAP. Mereka tidak diperkenankan menggunakan alat bukti lainnya sesuai keinginan mereka di luar jenis alat bukti yang telah ditentukan. Hanya alat-alat bukti yang telah ditetapkan tersebut yang dianggap sah dan



memiliki "kekuatan pembuktian". Penggunaan alat bukti di luar jenis yang telah ditetapkan tidak memiliki nilai pembuktian yang sah dan tidak diakui sebagai alat bukti yang mengikat. Namun, hal ini menimbulkan permasalahan dalam penggunaan alat bukti elektronik. Dalam Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagai suatu peraturan hukum khusus, terdapat prinsip-prinsip hukum baru yang berbeda dari sistem hukum yang ada dalam KUHP maupun KUHAP. Salah satunya adalah pengakuan alat bukti elektronik sebagai alat bukti yang sah dalam hukum pembuktian di Indonesia. Sejak UU ITE diundangkan, terjadi penambahan jenis alat bukti di persidangan, yaitu informasi elektronik dan/atau dokumen elektronik. Dalam ketentuan umum UU ITE, diketahui bahwa jenis data elektronik seperti tulisan, foto, suara, dan gambar dianggap sebagai informasi elektronik, sementara jenis informasi elektronik seperti tulisan, foto, suara, dan gambar yang disimpan pada flashdisk yang dapat dibuka melalui perangkat komputer dianggap sebagai dokumen elektronik.

Pasal 1 angka 4 UU ITE, dokumen elektronik merujuk pada data atau informasi yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau bentuk lain yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik. Dokumen elektronik meliputi tulisan, suara, gambar, peta, rancangan, foto, atau bentuk lainnya, serta mencakup huruf, tanda, angka, kode akses, symbol, atau perforasi yang memiliki makna atau arti dan dapat dipahami oleh orang yang mampu memahaminya. Sementara itu, pengertian informasi elektronik berdasarkan Pasal 1 angka 1 Undang-Undang ITE adalah satu atau kumpulan data elektronik, termasuk tulisan, suara, gambar, peta, rancangan, foto, elektronik data interchange (EDI), surat elektronik (electronic mail), telegram, telecopy, atau bentuk lainnya, serta mencakup huruf, tanda, angka, kode akses, symbol, atau perforasi yang telah diolah dan memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Dalam konteks Undang-Undang ITE, diatur bahwa informasi elektronik atau dokumen elektronik, beserta hasil cetaknya, merupakan alat bukti yang sah dan merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia. Alat bukti elektronik yang dibuat dalam bentuk informasi elektronik dan dokumen elektronik dianggap sah menurut UU ITE. Hal ini sejalan dengan Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yang menyatakan bahwa alat-alat bukti yang sah terdiri dari keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa.

Digital Forensik, juga dikenal sebagai komputer forensik, merupakan salah satu cabang ilmu forensik yang berfokus pada analisis bukti legal yang terdapat dalam komputer, perangkat elektronik, dan media penyimpanan digital lainnya. Menurut Marcella, digital forensik adalah kegiatan yang terkait dengan pengamanan, identifikasi, pengambilan/penyaringan, dan dokumentasi bukti digital dalam konteks kejahatan komputer. Metodologi ilmiah dalam Digital Forensik digunakan untuk mengidentifikasi, mencari, mengambil kembali, dan menganalisis barang bukti yang terdapat dalam perangkat teknologi tersebut. Tujuan utama dari digital forensik adalah untuk menyelidiki dan mengumpulkan bukti digital yang dapat digunakan dalam proses hukum. Para ahli digital forensik menggunakan berbagai teknik dan alat khusus untuk mengamankan data elektronik dan memastikan integritasnya agar dapat diakui secara sah di pengadilan. Hasil temuan dari analisis digital forensik kemudian disajikan sesuai dengan standar yang telah ditetapkan oleh pengadilan. Dengan demikian, bukti digital yang ditemukan oleh para ahli digital forensik memiliki nilai yang kuat dalam proses pengadilan dan membantu memastikan kebenaran dan keadilan dalam penanganan kasus. Berikut adalah berbagai jenis Digital Forensik:

a. Komputer Forensik

Komputer forensik merupakan jenis digital forensik yang memfokuskan pada penyidikan terhadap data yang berada atau terkait dengan komputer itu sendiri. Informasi mengenai layanan yang disediakan oleh komputer atau server biasanya tercatat dalam berbagai berkas log. Sebagai contoh, aktivitas pengguna yang gagal masuk karena salah memasukkan password akan tercatat sebagai bagian dari upaya untuk melakukan penerobosan akses dengan cara brute force password cracking. Selain itu, aktivitas seperti pengguna memasukkan flash disk ke port USB juga tercatat dan dapat menjadi fokus dalam penyidikan komputer forensik.

b. Jaringan Forensik

Jaringan forensik berfokus pada penyidikan terhadap data yang diperoleh melalui pengamatan pada jaringan. Contohnya, pengamat dapat mengamati lalu lintas data pada server-server yang diakses oleh seorang pengguna yang diduga melakukan penerobosan pada server tersebut. Perangkat khusus digunakan untuk melakukan penyadapan jaringan guna memantau dan mengumpulkan data terkait kejadian ini.

c. Aplikasi Forensik

Aplikasi forensik terkait dengan penyidikan terhadap penggunaan aplikasi tertentu. Aplikasi sering meninggalkan jejak sebagai bagian dari fungsi audit. Penyidik dapat memanfaatkan catatan jejak

tersebut, misalnya pada aplikasi email yang mencatat header email, untuk menelusuri kejadian yang terkait dengan email palsu atau email dengan maksud menyesatkan.

d. Mobile Forensik

Forensik jenis ini berkaitan dengan barang bukti elektronik seperti handphone dan smartphone. Pemeriksaan ini terfokus pada informasi digital yang tersimpan di perangkat tersebut, seperti panggilan masuk, panggilan keluar, SMS, e-mail, foto, dan video. Tujuan dari mobile forensik adalah untuk mengidentifikasi komunikasi antara pelaku kejahatan dan menganalisis data yang berkaitan dengan kejahatan yang terjadi.

e. Image Forensik

Forensik ini berkaitan dengan jenis barang bukti digital berupa file gambar. Jenis digital forensik ini sering dianalisis untuk mengetahui peralatan kamera digital yang digunakan untuk mengambil gambar tersebut dan juga dapat memeriksa waktu pengambilan gambar. Pemeriksaan ini dapat membantu dalam mengidentifikasi asal dan autentisitas gambar digital yang menjadi bukti dalam suatu kasus.

Digital Forensik terkait dengan tindak pidana penyebaran video asusila melalui media sosial Facebook adalah suatu proses penyelidikan dan analisis terhadap bukti digital yang terkait dengan tindakan kejahatan tersebut. Dalam kasus ini, bukti digital yang menjadi fokus adalah video asusila yang menyebar melalui platform media sosial Facebook. Proses digital forensik dimulai dengan :

1. Identifikasi bukti digital

video asusila yang menjadi objek kasus. Pihak penyidik akan mencari dan mengumpulkan data-data terkait video tersebut dari berbagai sumber, seperti perangkat elektronik, server media sosial, dan log aktivitas jaringan. Setelah berhasil mengidentifikasi video asusila yang relevan, langkah selanjutnya adalah melakukan proses penyimpanan bukti digital dengan hati-hati. Hal ini penting dilakukan agar integritas dan keaslian bukti tetap terjaga selama proses penyidikan berlangsung.

Proses penyimpanan harus dilakukan menggunakan perangkat dan metode yang aman, agar bukti tidak mengalami kerusakan atau perubahan yang dapat mempengaruhi keabsahannya di persidangan. Penyimpanan bukti digital juga melibatkan proses membuat salinan cadangan atau backup dari data asli, sehingga apabila terjadi kehilangan atau kerusakan pada bukti digital, masih ada salinan yang dapat digunakan untuk keperluan penyidikan lebih lanjut. Selain itu, dalam proses penyimpanan bukti digital, pihak penyidik harus menjaga kerahasiaan dan integritasnya dengan ketat, sehingga bukti tersebut tidak dapat diakses atau dimanipulasi oleh pihak yang tidak berwenang. Seluruh langkah dalam proses identifikasi dan penyimpanan bukti digital harus dilakukan dengan cermat dan sesuai dengan standar digital forensik yang berlaku. Hal ini bertujuan untuk memastikan bahwa bukti yang ditemukan dapat diakui sebagai alat bukti yang sah dan dapat digunakan dalam proses persidangan untuk menuntut pelaku kejahatan yang terlibat dalam penyebaran video asusila melalui media sosial Facebook.

2. Analisis bukti digital

Ahli digital forensik memiliki peran penting dalam analisis video asusila terkait tindak pidana penyebaran melalui media sosial Facebook. Proses analisis dilakukan secara mendalam dan terperinci untuk mengungkapkan berbagai informasi terkait video tersebut. Berikut adalah langkah-langkah dan teknik yang biasa dilakukan oleh ahli digital forensik dalam menganalisis video asusila:

a. Identifikasi Video

Ahli digital forensik akan melakukan identifikasi video asusila yang menjadi objek kasus. Video tersebut kemudian akan diperoleh dari berbagai sumber, seperti perangkat elektronik yang terlibat, server media sosial, atau salinan dari media yang menyimpannya.

b. Pemeriksaan Metadata

Metadata adalah informasi tambahan yang tersembunyi dalam file video, seperti tanggal dan waktu pembuatan, lokasi, kamera yang digunakan, dan perangkat yang menyimpannya. Ahli forensik akan memeriksa metadata ini untuk mengetahui asal usul dan pergerakan video tersebut.

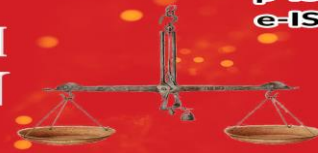
c. Analisis Alamat IP

Ahli digital forensik akan memeriksa alamat IP (Internet Protocol) yang terkait dengan penyebaran video asusila di platform Facebook. Alamat IP dapat membantu mengidentifikasi sumber dan lokasi pelaku penyebaran awal video.

d. Pengumpulan Bukti Elektronik

Proses analisis melibatkan pengumpulan bukti elektronik yang relevan, seperti log aktivitas jaringan, catatan server, dan riwayat perangkat yang terlibat dalam penyebaran video.

e. Analisis Perilaku Video



Ahli forensik akan memeriksa konten video untuk mengidentifikasi tanda-tanda manipulasi atau editing. Mereka juga akan mencari tanda-tanda pengeditan lainnya, seperti watermark atau tanda pengenal yang mungkin ada.

f. Penelusuran Penyebaran Video

Ahli forensik akan melakukan penelusuran dan analisis rute penyebaran video di platform Facebook dan jejaring sosial lainnya. Hal ini melibatkan identifikasi akun dan grup yang terlibat dalam penyebaran.

g. Pembuatan Laporan Forensik

Setelah analisis selesai, ahli digital forensik akan menyusun laporan forensik yang berisi hasil temuan, kesimpulan, dan rekomendasi. Laporan ini akan digunakan sebagai alat bukti di persidangan.

Faktor Yang Menjadi Penghambat Dalam Pembuktian Melalui Digital Forensik Terkait Tindak Pidana Penyebaran Video Asusila Melalui Media Sosial Facebook

Hukum pidana merupakan salah satu sarana yang dimiliki oleh negara dalam menjalankan kewajiban memberikan perlindungan pada hak setiap warga negara untuk mendapatkan rasa aman terutama terhadap ancaman terjadinya kejahatan. Jika dibandingkan dengan hukum yang lainnya, hukum pidana ini memiliki karakteristik yang khas, terletak pada adanya sanksi yang sangat tegas yaitu berupa nestapa. Oleh sebab itu, sistem hukum pidana harus selalu dievaluasi, direkonstruksi, diharmonisasikan dan diaktualisasikan secara cermat dan tepat, melalui pemahaman dan pemikiran yang utuh, agar di satu sisi handal dalam mengantisipasi perkembangan kejahatan, tetapi di sisi lain tidak mengancam hak asasi, harkat dan martabat manusia.

Hukum pidana saat ini dibutuhkan dalam menyelesaikan kejahatan yang semakin berkembang. Dalam hal ini misalnya tindak pidana cyber crime penyebaran video asusila melalui media sosial facebook seiring dengan berkembangnya teknologi. Pelaku tindak pidana cyber crime semakin pintar dalam melakukan aksinya, bahkan menghilangkan barang bukti agar tidak dapat diketahui. Hal tersebut dikarenakan barang bukti elektronik sangat mudah untuk diubah, dihapus dan dirusak. Tindak pidana cyber crime sangat meresahkan masyarakat, termasuk masyarakat. Masih banyak masyarakat yang enggan melaporkan ke pihak yang berwajib ketika menjadi korban tindak pidana cyber crime. Adapun prosedur untuk menuntut secara pidana terhadap tindak pidana siber, secara sederhana dapat dijelaskan sebagai berikut: korban yang merasa haknya dilanggar atau dirugikan, setelah proses penyidikan selesai, maka berkas perkara oleh Penyidik akan dilimpahkan kepada Penuntut Umum untuk dilakukan penuntutan di muka pengadilan.

Berdasarkan wawancara dengan Brigadir Fahrul Anggara Putra, S.Pd,M.H, CEH, CHFI, banit Subdit Siber menjelaskan bahwa keengganan masyarakat yang menjadi korban tindak pidana cyber crime penyebaran video asusila melalui media sosial facebook kepada pihak yang berwajib dikarenakan sulitnya kasus tersebut terungkap. Selain itu korban kurang dalam mengumpulkan bukti awal yang cukup. Di sisi lain apa yang dialaminya, menganggap bahwa itu adalah aib karena kurang berhati-hati dalam memanfaatkan teknologi, dan lain sebagainya. Sehingga malu jika harus melapor ke pihak yang berwajib dan diketahui oleh orang banyak.

Penyidikan tindak pidana cyber crime penyebaran video asusila melalui media sosial facebook menggunakan digital forensik dalam penerapannya tidak dapat berjalan sebagaimana mestinya. Hal tersebut juga dialami oleh Subdit Siber Ditreskrimsus Polda Kalimantan Barat yang mengalami hambatan dalam menerapkan digital forensik terhadap penyidikan tindak pidana cyber crime penyebaran video asusila. Berdasarkan wawancara dengan Brigadir Fahrul Anggara Putra, S.Pd,M.H, CEH, CHFI, bahwa hambatan-hambatan dalam menerapkan digital forensik terhadap penyidikan tindak pidana cyber crime penyebaran video asusila terbagi menjadi dua, yaitu :

1. Hambatan Internal, terdiri dari

a. Kualitas Penyidik

Penyidik Kepolisian memiliki peran penting dalam upaya penanggulangan tindak pidana cyber crime penyebaran video asusila melalui media sosial facebook, dimana kemampuan atau kualitas Penyidik di setiap unit harus memadai dan diperhatikan karena sangat berpengaruh untuk mengungkap kasus-kasus tindak pidana cyber crime penyebaran video asusila melalui media sosial facebook yang dilaporkan oleh masyarakat. Adanya Subdit Siber di lingkungan Kepolisian membuktikan bahwa dibutuhkannya Penyidik khusus yang memiliki kemampuan di bidang informasi dan transaksi elektronik, guna menangani kejahatan-kejahatan dunia maya secara maksimal. Pada instansi Kepolisian, khususnya subdit Siber yang ada di setiap Polda di Indonesia, khususnya subdit Siber kualitas Penyidik masih banyak masalah. Hal ini dikarenakan belum adanya pendidikan khusus untuk para calon-calon Penyidik cyber crime yang memberikan pengetahuan terkait cyber crime, khususnya menangani masalah dan cara kerja yang profesional dalam melakukan penanggulangan terhadap

tindak pidana cyber crime. Penyidik pada Subdit Siber belum ada yang memiliki sertifikasi program Certified Ethical Hacker (CEH) dan sertifikasi program Computer Hacking Forensic Investigator Certification (CHFI) untuk melakukan pemeriksaan barang bukti digital di laboratorium digital forensik.

b. Jumlah Personil Penyidik

Khususnya pada Subdit Siber, terdapat kekurangan kuantitas atau jumlah Penyidik yang tersedia. Keterbatasan jumlah personil Penyidik ini menghadirkan masalah, terutama karena tidak sebanding dengan tingginya jumlah laporan atau aduan yang masuk dari masyarakat terkait kasus-kasus cyber crime. Hal ini berdampak pada lambatnya penanganan kasus oleh Kepolisian.

Berdasarkan wawancara dengan Brigadir Fahrul Anggara Putra, S.Pd, M.H, CEH, CHFI, terungkap bahwa laporan mengenai tindak pidana cyber crime, khususnya penyebaran video asusila melalui media sosial seperti Facebook, sangatlah banyak. Namun, jumlah kasus yang berhasil diproses oleh pihak Kepolisian hanya sedikit bahkan setiap tahunnya hanya satu kasus. Hal ini disebabkan karena korban seringkali kesulitan untuk menunjukkan bukti awal yang cukup untuk mendukung pengusutan kasus ini. Masalah lain yang dihadapi oleh pihak Kepolisian adalah kesulitan dalam mencari bukti yang cukup, karena terbatasnya jumlah personel Penyidik dan keterbatasan kemampuan mereka dalam menghadapi kasus-kasus kompleks yang terkait dengan teknologi. Akibatnya, proses pengumpulan dan analisis bukti seringkali membutuhkan waktu yang cukup lama.

Keterbatasan jumlah Penyidik dan kemampuan teknis mereka menjadi tantangan serius dalam menangani kasus cyber crime yang semakin meningkat. Diperlukan langkah-langkah yang lebih efektif dalam meningkatkan kapasitas Subdit Siber untuk dapat lebih cepat dan efisien dalam menangani kasus-kasus seperti penyebaran video asusila melalui media sosial dan melawan ancaman cyber crime secara lebih luas.

c. Lamanya Hasil dari Proses Digital Forensik

Keterbatasan jumlah Penyidik menyebabkan setiap penyidik harus menunggu dalam antrian untuk menggunakan laboratorium digital forensik. Karena laboratorium digital forensik hanya ada di Subdit Siber setiap Provinsi, maka setiap kasus yang membutuhkan analisis forensik komputer harus mengikuti antrian tersebut. Hal ini menyebabkan waktu yang cukup lama dibutuhkan untuk menyelesaikan setiap kasus. Ketika terjadi kasus tindak pidana cyber crime, seperti penyebaran video asusila melalui media sosial Facebook, permintaan untuk analisis forensik komputer semakin meningkat. Namun, karena keterbatasan laboratorium digital forensik yang ada, setiap kasus harus menunggu giliran untuk dianalisis, sehingga prosesnya menjadi lebih lambat.

Selain itu, karena keterbatasan personel di Subdit Siber, Penyidik harus bergantian dengan Polres lainnya yang juga membutuhkan jasa laboratorium digital forensik. Hal ini memperpanjang waktu penyelesaian kasus, mengingat setiap Polres hanya memiliki akses terbatas ke laboratorium digital forensik di setiap Provinsi.

Penanganan kasus tindak pidana cyber crime memiliki batas waktu maksimal yaitu 120 hari, sebagaimana diatur dalam ketentuan hukum. Oleh karena itu, keterbatasan waktu tersebut menjadi tantangan serius bagi Subdit Siber dan Penyidik dalam menangani kasus-kasus yang semakin marak terjadi seperti penyebaran video asusila melalui media sosial. Upaya untuk meningkatkan kapasitas laboratorium digital forensik dan jumlah personel yang berkualifikasi perlu dilakukan untuk memastikan penanganan kasus cyber crime yang lebih efektif dan efisien.

d. Sarana dan Prasarana

Mengungkap kasus cyber crime dibutuhkan sarana dan prasarana yang menunjang kinerja Penyidik. Sarana dan prasarana tersebut berupa laboratorium digital forensik yang digunakan untuk mengungkap data-data bersifat digital, serta merekam dan menyimpan bukti-bukti berupa soft copy (gambar, program, html, suara dan lain sebagainya). Tujuan lainnya adalah untuk mengamankan dan menganalisis bukti digital, serta memperoleh berbagai fakta yang objektif, yang dapat digunakan menjadi bukti dalam proses hukum. Melalui digital forensik, Penyidik dapat mengetahui siapa saja orang yang mengirim email, kapan dan dimana keberadaan alamat pengirim berdasarkan server pengirim. Berdasarkan wawancara dengan Brigadir Fahrul Anggara Putra, S.Pd, M.H, CEH, CHFI.

2. Hambatan eksternal, terdiri dari :

a. Aspek Masyarakat

Kurangnya pemahaman dari masyarakat tentang pengertian tindak pidana cyber crime, khususnya penyebaran video asusila melalui media sosial Facebook, merupakan salah satu tantangan utama dalam penanganan kasus ini. Mayoritas dari masyarakat yang terlibat atau menjadi korban dari tindak



pidana cyber crime tersebut merasa malu atau khawatir akan mendapatkan sanksi sosial secara tidak langsung di lingkungannya jika melapor ke pihak yang berwajib.

Perasaan malu atau takut ini menyebabkan banyak dari mereka enggan untuk melaporkan kejadian tersebut ke pihak Kepolisian. Dampak dari ketidakmampuan masyarakat untuk melapor ini menyulitkan pihak Kepolisian untuk mengetahui sejauh mana kasus tindak pidana cyber crime penyebaran video asusila melalui media sosial Facebook menyebar di masyarakat. Karena informasi terbatas tentang kasus-kasus yang sebenarnya terjadi, penanganan tindak pidana cyber crime ini menjadi terhambat. Pihak Kepolisian kesulitan untuk melakukan upaya pencegahan atau penanggulangan secara tepat dan efisien. Upaya untuk meningkatkan kesadaran masyarakat mengenai tindak pidana cyber crime serta memberikan perlindungan dan keamanan bagi para pelapor merupakan langkah penting untuk mengatasi masalah ini. Pihak berwenang harus bekerja lebih keras untuk menciptakan lingkungan yang aman bagi masyarakat agar mereka merasa nyaman melaporkan kejahatan cyber yang mereka alami tanpa rasa malu atau takut mendapatkan sanksi sosial.

b. Aspek Yuridis

Penerapan digital forensik dalam penyidikan tindak pidana cyber crime penyebaran video asusila melalui media sosial Facebook saat ini belum diatur secara spesifik dalam peraturan perundang-undangan. Sebagai akibatnya, pihak Kepolisian belum memiliki landasan hukum dan pedoman yang jelas untuk menerapkan digital forensik dalam penyidikan kasus-kasus tersebut. Peraturan UU ITE yang ada saat ini hanya mengatur mengenai alat bukti informasi dan transaksi elektronik, bukan mengenai digital forensik secara menyeluruh. Pentingnya pengaturan terkait digital forensik dalam pembuktian dapat dijelaskan sebagai berikut:

- a) Sebagai acuan bagi aparat penegak hukum dalam menangani barang bukti dan alat elektronik yang terkait dengan tindak pidana cyber crime. Dengan pengaturan yang jelas, aparat penegak hukum dapat menggunakan digital forensik secara efektif dan tepat dalam proses penyidikan dan pengumpulan bukti.
- b) Meningkatkan kredibilitas barang bukti dan alat bukti elektronik yang digunakan dalam persidangan. Dengan adanya pengaturan yang sesuai, keabsahan dan integritas bukti digital dapat dipertanggungjawabkan dengan jelas di hadapan pengadilan.
- c) Menghindari terjadinya kekosongan yuridis atau kekosongan hukum dalam pengaturan tata cara pembuktian tindak pidana siber (cybercrime). Dengan adanya ketentuan yang mengatur tentang digital forensik, akan tercipta kerangka hukum yang lengkap dan dapat mendukung efektivitas penanganan kasus cyber crime.

c. Aspek Barang Bukti Digital dan Alat Bukti

Barang bukti yang terkait dengan tindak pidana cyber crime memiliki perbedaan dengan tindak pidana umum, karena sasaran atau media dalam cyber crime adalah data atau sistem elektronik yang terhubung ke internet. Barang bukti dalam kasus cyber crime biasanya berupa format digital. Kondisi ini menyebabkan barang bukti mudah diubah, dihapus, atau disembunyikan oleh pelaku kejahatan cyber. Karena sifat digitalnya, alat bukti dalam tindak pidana cyber crime cenderung lebih sulit ditemukan dibandingkan dengan alat bukti dalam tindak pidana umum. Perbedaan ini menjadikan proses penanganan kasus cyber crime menjadi lebih kompleks. Selain itu, dalam kasus tindak pidana umum, saksi-saksi biasanya berada di lokasi atau tempat yang sama dengan korban dan/atau pelaku. Namun, dalam tindak pidana cyber crime, saksi-saksi seringkali tidak berada di lokasi yang sama, bahkan mungkin berada di luar daerah atau negara.

Kehadiran saksi menjadi sangat penting dalam proses penegakan hukum, terutama dalam kasus tindak pidana cyber crime. Namun, keterbatasan akses fisik terhadap saksi yang berada di luar daerah atau negara menyulitkan Penyidik dalam melakukan pemeriksaan dan pemberkasan. Permasalahan ini menjadi tantangan serius dalam menangani kasus cyber crime, karena memerlukan kerjasama lintas negara dan penggunaan teknologi yang canggih untuk mengumpulkan bukti dan menyelidiki kasus secara efektif.

Upaya Yang Telah Dilakukan Dalam Optimalisasi Pembuktian Digital Forensik Terkait Tindak Pidana Penyebaran Video Asusila Melalui Facebook

Penyalahgunaan teknologi informasi telah menjadi agenda kejahatan di tingkat global. Kejahatan ini menjadi ujian berat bagi masing-masing negara untuk menghadapinya. Salah satu alat yang digunakan oleh negara untuk melawannya adalah hukum. Hukum berfungsi untuk mencegah terjadinya dan menyebarnya cyber crime, serta menindak pelaku jika terbukti telah merugikan masyarakat dan negara. Negara hukum menentukan perangkat-perangkat hukum yang beroperasi sesuai dengan

peraturan yang telah ditetapkan sebelumnya. Tindakan yang dilakukan oleh aparat penegak hukum ini merupakan implementasi hukum.

Alat negara (penegak hukum) bertanggung jawab untuk menggunakan hukum sebagai senjata dalam melawan berbagai bentuk kejahatan yang mengancam bangsa Indonesia. Penegak hukum dituntut untuk bekerja keras menghadapi perkembangan cyber crime yang semakin mengkhawatirkan dan meresahkan masyarakat. Perlindungan hukum adalah upaya yang harus dilakukan oleh aparat penegak hukum untuk memberikan rasa aman bagi masyarakat dari gangguan dan ancaman yang berasal dari berbagai pihak. Perlindungan hukum merupakan hak asasi manusia dalam melakukan berbagai aktivitas.

Penanganan dan penyitaan barang bukti serta alat bukti elektronik dalam kasus tindak pidana cyber crime, seperti penyebaran video asusila, harus autentik dan dapat direpresentasikan agar tidak rusak. Namun, dalam penerapan digital forensik untuk penyidikan tindak pidana cyber crime penyebaran video asusila, terdapat beberapa hambatan yang dihadapi oleh Penyidik. Oleh karena itu, hambatan-hambatan tersebut harus segera diatasi untuk memastikan penyidikan berjalan dengan efektif dan efisien. Menurut wawancara dengan Brigadir Fahrul Anggara Putra, S.Pd, M.H, CEH, CHFI, Subdit Siber Polda Kalbar telah melakukan upaya untuk mengatasi hambatan dalam penerapan digital forensik dalam penyidikan kasus tindak pidana cyber crime penyebaran video asusila.

a. Upaya untuk mengatasi hambatan internal

- 1) Penyidik Subdit Siber Polda Kalimantan Barat (Kalbar) melaksanakan pelatihan sertifikasi bagi para penyidik di bidang informasi dan transaksi elektronik.

Tujuan utama dari pelatihan ini adalah memberikan pengetahuan yang memadai dan meningkatkan kemampuan Penyidik dalam melakukan penyidikan terhadap kasus cyber crime. Pelatihan ini dirancang untuk memastikan bahwa para Penyidik memiliki pemahaman mendalam tentang teknologi informasi dan transaksi elektronik yang terkait dengan kejahatan siber. Selain pelatihan sertifikasi, juga diadakan Pendidikan Kejuruan (Dikjur) dan Pendidikan Pengembangan (Dikbang) untuk para Penyidik. Tujuan dari program pendidikan ini adalah untuk meningkatkan kompetensi dan keahlian Penyidik dalam menghadapi tantangan yang berkaitan dengan perkembangan teknologi dan metode cyber crime yang semakin kompleks. Dikjur dan Dikbang memberikan kesempatan kepada para Penyidik untuk memperdalam pengetahuan mereka dalam bidang khusus seperti digital forensik, keamanan siber, dan analisis data elektronik.

- 2) Menambah jumlah personil Penyidik dalam Subdit Siber Polda Kalbar. Hal ini bertujuan untuk memperkuat tim penyidik dan meningkatkan efektivitas penanganan kasus cyber crime.
- 3) Mengusulkan kepada pimpinan tertinggi Kepolisian untuk menyediakan laboratorium digital forensik di setiap Polda. Tujuannya adalah agar penyidikan tindak pidana cyber crime dapat berjalan dengan lebih efektif dan efisien tanpa perlu melakukan perjalanan jauh ke Polda lain. Dengan adanya laboratorium digital forensik di setiap Polda, diharapkan lebih banyak kasus tindak pidana cyber crime penyebaran video asusila melalui media sosial Facebook dapat terselesaikan dengan cepat dan tepat.

b. Upaya untuk mengatasi hambatan eksternal:

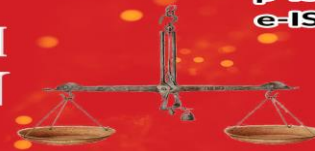
- 1) Subdit Siber Polda Kalimantan Barat (Kalbar) melakukan penyuluhan dan sosialisasi kepada masyarakat tentang kejahatan yang semakin berkembang, termasuk cyber crime.

Penyuluhan dan sosialisasi ini bertujuan untuk meningkatkan kesadaran dan pemahaman masyarakat tentang potensi bahaya dan risiko yang dapat dihadapi saat beraktivitas di dunia maya. Selama penyuluhan dan sosialisasi, para penyidik memberikan informasi yang relevan tentang berbagai bentuk cyber crime yang sering terjadi, seperti penyebaran video asusila melalui media sosial Facebook. Masyarakat diberikan wawasan tentang teknik-teknik umum yang digunakan oleh para pelaku kejahatan untuk mencuri data pribadi, menyebarkan konten ilegal, atau melakukan penipuan online. Dengan meningkatkan pemahaman tentang cyber crime, diharapkan masyarakat akan menjadi lebih waspada dan berhati-hati dalam beraktivitas di dunia maya. Mereka dapat mengenali potensi bahaya dan tanda-tanda ancaman cyber crime, sehingga dapat mengambil langkah-langkah pencegahan yang tepat. Selain itu, masyarakat juga diinformasikan tentang cara melaporkan tindak pidana cyber crime kepada pihak berwajib agar dapat ditindaklanjuti dengan tepat.

Melalui penyuluhan dan sosialisasi, Subdit Siber Polda Kalbar berusaha membentuk kesadaran kolektif dalam masyarakat untuk bersama-sama melawan kejahatan siber. Dengan menjadi "polisi" untuk diri sendiri, masyarakat dapat membantu memitigasi risiko cyber crime dan menciptakan lingkungan maya yang lebih aman dan bertanggung jawab bagi seluruh penggunanya.

- 2) Melakukan kerjasama dengan provider dan Kementerian Kominfo.

Kerjasama ini bertujuan untuk saling memanfaatkan perangkat dan sumber daya yang lebih lengkap dari kedua instansi terkait dalam rangka melakukan pengungkapan kasus cyber crime. Dengan



bekerja sama, keduanya dapat saling melengkapi keahlian, teknologi, dan peralatan yang diperlukan untuk menghadapi tantangan yang kompleks dari kejahatan siber. Selain kerjasama, diperlukan pembentukan peraturan khusus yang mengatur tentang digital forensik. Peraturan ini bertujuan untuk memberikan pedoman yang jelas bagi para penyidik dalam melakukan identifikasi, pengumpulan, akuisisi, dan pemeliharaan bukti digital yang diperoleh dari tempat kejadian perkara atau perangkat elektronik terkait. Dengan adanya peraturan yang mengatur digital forensik, para penyidik memiliki panduan baku yang harus diikuti dalam proses investigasi, sehingga dapat menghindari kesalahan dan memastikan keabsahan serta otentisitas bukti yang dihadirkan dalam persidangan. Pentingnya peraturan yang mengatur digital forensik adalah untuk menjaga kualitas dan integritas bukti digital yang digunakan dalam proses hukum. Hal ini akan membantu memastikan bahwa hasil analisis forensik terhadap bukti elektronik dapat dipertanggungjawabkan secara ilmiah dan sah di mata hukum. Dengan begitu, kasus-kasus cyber crime dapat ditangani secara efektif dan adil, dan pelaku kejahatan tidak dapat mengelak atau meragukan keabsahan bukti yang digunakan oleh aparat penegak hukum.

KESIMPULAN DAN SARAN

Kesimpulan

1. Penerapan digital forensik melibatkan beberapa tahapan penting, di antaranya identifikasi bukti digital, penyimpanan bukti digital, analisis bukti digital, dan presentasi hasil temuan. Digital forensik memiliki peran krusial dalam melakukan pembuktian dalam kasus-kasus hukum. Di Indonesia, sistem pembuktian mensyaratkan minimal dua alat bukti yang sah dan keyakinan dari Hakim untuk menentukan kesalahan terdakwa. Dalam kasus tindak pidana cyber crime, alat bukti elektronik harus memenuhi persyaratan baik secara formil maupun materiil agar dianggap sah dan dapat diterima di persidangan. Oleh karena itu, penerapan digital forensik dalam penyidikan tindak pidana cyber crime, khususnya penyebaran video asusila, memiliki peran penting dalam menemukan alat bukti dan barang bukti elektronik yang relevan untuk proses peradilan.
2. Subdit Siber Polda Kalbar menghadapi berbagai hambatan dalam menerapkan digital forensik dalam penyidikan tindak pidana cyber crime penyebaran video asusila. Hambatan-hambatan tersebut dapat dikategorikan menjadi dua, yaitu hambatan internal dan hambatan eksternal.

Saran

1. Subdit Siber Polda Kalbar mengadakan pelatihan di bidang informasi dan transaksi elektronik yang bersertifikasi bagi para Penyidik. Selain itu, mereka juga menyelenggarakan Pendidikan Kejuruan (Dikjur) dan Pendidikan Pengembangan (Dikbang) untuk meningkatkan kemampuan dan kompetensi para Penyidik dalam menghadapi kasus cyber crime. Selain itu, upaya dilakukan dengan menambah jumlah personil Penyidik untuk memperkuat tim penyidik dalam menangani laporan dan kasus-kasus yang masuk.
2. Selanjutnya, Subdit Siber Polda Kalbar berupaya menyediakan laboratorium digital forensik di setiap Polres untuk memfasilitasi proses penyidikan dan analisis bukti digital dengan lebih efisien. Penyuluhan dan sosialisasi kepada masyarakat tentang bahaya dan dampak dari kejahatan cyber crime, agar masyarakat lebih waspada dan proaktif dalam melaporkan kasus-kasus yang terjadi. Selain itu, mereka menjalin kerjasama dengan provider dan Kementerian Kominfo guna memanfaatkan perangkat dan sumber daya yang lebih lengkap dalam mengungkap kasus cyber crime.

DAFTAR PUSTAKA

- Andi Sofyan, 2013, Hukum Acara Pidana Suatu Pengantar, Yogyakarta: Rangkang Education.
Didik Suyatna, 2015, Belajar Mengenal Forensika Digital, Kelompok Penerbit Diandra, Yogyakarta.
Imam Riadi, 2022, Digital Forensik, Yogyakarta, Diandra Kreatif, hal.1
Muhammad Nuh Al-Azhar, 2012, Digital Forensic: Panduan Praktis Investigasi Komputer, Jakarta, Salemba Infotek.
Yahya Harahap. 2007. Permasalahan, dan Penerapan KUHP: Pemeriksaan Sidang Pengadilan Banding, Kasasi, dan Peninjauan Kembali. Jakarta: Sinar Grafika.
Abdullah Labib. Kejahatan Mayantara. Re-fika Aditama. Bandung. 2005.
Adami Chazawi, Pelajaran Hukum Pidana Bagian 1, (Jakarta: Raja Grafindo Persada), 2002.
Agus Raharjo. Cyber Crime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi. Citra Aditya Bakti. Bandung. 2002.

Ahmad M. Ramli. *Cyber Law dan HaKi*. Re-fika Aditama. Bandung. 2004

Al Wisnubroto. *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*. Universitas Widyatama. Yogyakarta . 1999.

Andi Hamzah. *Hukum Acara Pidana Indonesia*. CV Sapta Arta Jaya. Jakarta. 1996.

Anthon F. Susanto. *Wajah Peradilan Kita : Konstruksi Sosial Tentang Penyimpangan, Mekanisme Kontrol dan Akuntabilitas Peradilan Pidana*. Refika Aditama. Bandung. 2004

Dikdik M Arief Mansur dan Elisatris Gultom. *Cyber Law Aspek Hukum Teknologi Informasi*. Refika Aditama. Bandung. 2005.

Edmon Makarim. *Pengantar Hukum Telematika*. PT.Raja Grafindo Persada. Jakarta. 2005.

_____, *Tindak Pidana terkait dengan Komputer dan Internet Suatu Kajian Pidana Materil dan Formil*. Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia, FHUI, Jakarta. 2005

Hartanti, Evi, *Tindak Pidana Korupsi*, (Jakarta: Sinar Grafika), 2005.

HMA. *Kuffal, Tata Cara Penggeledahan dan Penyitaan*, (Malang : UMM Press), 2005.

I Wayan Parthiana. *Hukum Pidana Internasional*. Yrama Widia. Bandung. 2006.

_____, *Hukum Pidana Internasional dan Ekstradisi*. Yrama Widia. Bandung. 2004.

Jan smith. *Komputer : Suatu tantangan baru di bidang hukum*". Airlangga University Press. Surabaya. 1991.

Lamintang. *Hukum Pidana*. Citra Aditya. Bandung. 1992

_____, *Dasar-Dasar Hukum Pidana Indonesia*, PT. Citra Aditya Bakti, , Band-ung, 1996

Muladi dan Barda Nawawi Arief, *Teori-Teori Kebijakan Pidana*, (Bandung: Alumni), 1984.

Mohammad Taufik Makarao, Suhasril, *Hukum Acara Pidana dalam Teori dan Praktek*, (Jakarta: Ghalia Indonesia), 2004

Moeljatno, *Asas-asas Hukum Pidana*, (Jakarta: Rineka Cipta), 1993.

Mochtar Kusumaatmadja. *Hukum, Masyarakat, Dan Pembinaan Hukum Na-sional*. Bina Cipta. Bandung. 1976.

_____. *Konsep-Konsep Hukum dalam pembangunan*. Alumni. Bandung. 2002.

Munir Fuady. *Teori Hukum Pembuktian (Pidana dan Perdata)*. Citra Aditya Bhakti. Jakarta. 2006.

M. Hamdan, *Tindak Pidana Suap dan Money Politics*, (Medan: Pustaka Bangsa Pers), 2005.

M. Arsyad Sanusi, *Hukum dan Teknologi Informasi*, (Jakarta: Tim Kemas Buku), 2005.

M. Yahya Harahap. *Pembahasan Perma-salahan dan Penerapan KUHAP : Penyidikan dan Penuntutan*. Sinar Grafika. Jakarta. 2003.

_____. *Pembahasan Permasalahan dan Penerapan KU-HAP :Pemeriksaan SidangPengadi-lan, Banding, Kasasi dan Penin-jauan Kembali*. Sinar Grafika. Ja-karta.2003.

Otje Salman S.dan Anthon F. Susanto. *Teori Hukum:Mengingat, Mengumpulkan, dan membuka Kembali*. Refika Adi-tama. Bandung. 2004.

Sitompul, Asril, *Hukum Internet, Pengenalang Mengenai Masalah Hukum di Cyberspace*, Citra Aditya Bakti, Bandung, 2001.

Soeharto. *Hukum Pidana Materil* . Gramedia Pustaka Utama. Jakarta. 1997

Sudarto. *Kapita Selektta Hukum Pidana*. Alumni. Bandung. 1986.

Wirjono Prodjodikoro, *Asas-asas Hukum Pidana di Indonesia*, (Bandung: Refika Aditama), 2003.

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (ITE)

Undang-Undang Nomor 4 tahun 2004 Tentang Pokok-Pokok Kekuasaan Ke-hakiman

<http://www.legalitas.com>

<http://www.bphn.go.id>

http://www.taufik.staff.ugm.ac.id/images/file/kuliah_4.pdf

Hasil Wawancara Personil Subdit Siber Polda Kalbar Brigadir Fahrul Anggara Putra, S.Pd, M.H, CEH, CHFI