



Volume 2 Nomor 1, Agustus 2021: h. 8-16

E-ISSN: 2775-9407



Lisensi Creative Commons Atribusi-Non Commercial 4.0 Internasional

Pulsa Data Internet Sebagai Barang Bukti Pencurian

Erwin Ubwarin^{1*}

¹Fakultas Hukum Universitas Pattimura, Ambon, Indonesia.

E-mail Korespondensi : eubwarin@gmail.com^{1*}

Dikirim:	Direvisi:	Dipublikasi:
Info Artikel	Abstract	
Keywords: Internet Data Credit, Evidence, Electronic	<i>The purpose of this study is to analyze and find internet data pulses as evidence of the crime of theft, this research method uses normative juridical research methods, and the results of internet data pulse research are electronic evidence, and can be brought before the court to be assessed for validity, this is in accordance with Article 44 of Law Number 11 of 2008 concerning Information and Electronic Transactions, the expansion of this evidence is also seen in the case of "electrical arrest" in 1921, Hoge Raad enforces article 310 NWvS (Article 362 of the Criminal Code) which clearly refers to the term "goods" (goed) in the formulation of the rules.</i>	
Kata Kunci: Pulsa Data Internet, Bukti, Elektronik	Abstrak	
DOI: Xxxxxxx	<i>tujuan penelitian ini untuk menganalisis dan menemukan pulsa data internet sebagai alat bukti tindak pidana pencurian, metode penelitian ini menggunakan metode penelitian yuridis normatif, dan hasil penelitian pulsa data internet merupakan barang bukti elektronik, dan dapat dibawa ke hadapan pengadilan untuk dinilai keasahannya, hal ini sesuai dengan Pasal 44 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, perluasan barang bukti ini juga terlihat dalam kasus "arrest listrik" tahun 1921, Hoge Raad memberlakukan pasal 310 N.W.v.S. (pasal 362 KUHP) yang secara jelas menunjuk istilah "barang" (goed) di dalam rumusan kaidahnya..</i>	

1. Pendahuluan

Perkembangan teknologi informasi dengan kehadiran internet membuat ruang dan waktu terasa dekat, dan tidak memakan biaya, ketika pandemi Covid 19 datang perkembangan internet lebih cepat karena dengan pembatasan sosial, orang lebih banyak bersilahturahmi lewat media sosial yang dibantu dengan jaringan internet. Facebook, MeChat, Instagram, Tiktok, dan berbagai platform media sosial berkembang pesat. Sedangkan pada sisi perkembangan hukum teknologi dan informasi berdampak terhadap masyarakat secara umum dan terjadi dalam segala sektor kehidupan. Berdasarkan hal tersebut, semakin maju dan tinggi tingkat kemampuan berpikir seseorang atau bangsa, akan semakin maju dan tinggi pula ilmu pengetahuan dan teknologi yang dikuasainya.¹ Perkembangan kejahatan juga semakin berkembang dari konvensional sampai dengan memakai teknologi untuk melakukan kejahatan.

Pada saat pandemi Covid-19, beberapa orang beraktifitas dan bekerja dari rumah, ditangan manusia ada *smart phone* yang membuat orang dapat rapat sambil masak, mengikuti kegiatan di beberapa tempat dengan beberapa perangkat *smart phone* yang terkoneksi dengan internet, selain *sim card* di smart yang dapat memberikan akses internet, ada juga *Wireless Fidelity* (WiFi). Wi-fi memiliki sistem keamanan yang berfungsi untuk mencegah orang yang tidak berhak mengakses jaringan Wi-fi tersebut. Sistem keamanan tersebut yaitu;

1. WEP (*Wired Equivalent Privacy*)

WEP merupakan standar keamanan dan enkripsi pertama yang digunakan pada *wireless*, WEP terdiri dari dua tingkatan yakni kunci 64 bit, dan 128 bit. Sebenarnya kunci rahasia pada kunci WEP 64 bit hanya 40 bit, sedangkan 24 bit merupakan Inisialisasi Vektor (IV). demikian juga pada kunci WEP 128 bit, kunci rahasia terdiri dari 104 bit.

2. WPA-PSK atau WPA2-PSK

WPA merupakan teknologi keamanan sementara yang diciptakan untuk mengganti kunci WEP. Ada dua jenis yakni WPA personal (WPA-PSK) dan WPA-RADIUS.

3. MAC Filtering

Mac Filtering merupakan metode keamanan yang menyaring Mac address tertentu saja yang dapat terhubung dengan perangkat wi-fi.

4. Captive Portal

Infrastruktur *Captive Portal* awalnya didesain untuk keperluan komunitas yang memungkinkan semua orang dapat terhubung (*open network*). Namun sekarang *Captive Portal* dimanfaatkan oleh penyedia warnet yang berbasis Wi-Fi. *Captive Portal* sebenarnya merupakan mesin *router* atau *gateway* yang memproteksi atau tidak mengizinkan adanya trafik hingga user melakukan registrasi/otentikasi.

¹ Abdulkadir Muhammad, *Kajian Hukum Pidana Ekonomi*, PT. Citra Aditya Bakti, Bandung, 2001, hlm.9.

Penelitian yang dilakukan Baihaqi, Yeni Yanti, Zulfan, menemukan Teknologi jaringan wireless saat ini berkembang sangat pesat terutama dengan hadirnya perangkat teknologi informasi dan komunikasi. Komputer, *notebook*, PDA, telepon seluler (*handphone*) dan periferal lainnya mendominasi pemakaian teknologi jaringan wireless. Penggunaan teknologi jaringan wireless yang di implementasikan dalam suatu jaringan lokal sering dinamakan WLAN (*Wireless Local Area Network*). Teknologi jaringan wireless memanfaatkan frekuensi tinggi untuk menghantarkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat komunikasi yang di gunakan oleh user maupun oleh operator yang memberikan layanan komunikasi. Namun dengan adanya user yang memanfaatkan teknologi jaringan WiFi, maka dapat memberikan sedikit celah keamanan kepada penyerang, sehingga penyerang dapat mengetahui password keamanan WPA2-PSK pada saat user terhubung ke jaringan WiFi. Kelemahan jaringan wireless secara umum dapat dibagi menjadi dua jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Secara garis besar, celah pada jaringan wireless terbentang di atas empat layer di mana keempat lapis layer tersebut sebenarnya merupakan proses terjadinya komunikasi data pada media wireless. Keamanan sistem jaringan wireless menjadi suatu keharusan untuk lebih diperhatikan, karena jaringan internet yang sifatnya publik dan global pada dasarnya tidak aman. Adanya lubang-lubang keamanan pada sistem jaringan menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan para hacker, cracker dan script kiddies untuk memanfaatkan pengaksesan jaringan secara bebas, pembobolan password keamanan pada jaringan wireless, dan lain-lain. Oleh karena itu, penulis ingin mengimplementasikan sistem keamanan WPA2-PSK pada jaringan WiFi untuk mengetahui password WPA2-PSK melalui user yang terhubung ke jaringan WiFi.²

Tahapan Pembobolan Wifi, Tahapan pertama adalah Pengumpulan bahan, mencari tutorial - tutorial baik dari internet, buku dan artikel - artikel tentang masalah yang berhubungan dengan keamanan jaringan wireless, Tahapan kedua Menyiapkan *hardware* dan *software* yang dibutuhkan seperti menggunakan terminal Kali Linux dan *tool-tool* tambahan lainnya untuk proses penyerangan. Tahapan ketiga Melakukan konfigurasi *tools* yang telah tersedia pada Kali Linux ataupun tool tambahan lainnya agar proses penyerangan terhadap *client* dapat berjalan dengan baik. Tahapan keempat Menunggu user yang terkoneksi ke internet untuk mendapatkan handshake ataupun informasi mengenai *SSID*, *MAC address*, *IP address*, *Channel* dan lain-lain. Sehingga diperoleh sebuah paket berupa kode enkripsi untuk dipecahkan menjadi password WPA2-PSK. Tahapan kelima *User attack* dapat mengakses jaringan WiFi dengan memanfaatkan handshake dan paket kode enkripsi yang telah dipecahkan dengan menggunakan *tools* pada Kali Linux, jika *handshake* sulit

² Baihaqi, Yeni Yanti, Zulfan, Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi, Serambi Engineering, Volume III, No.1, Januari 2018

untuk didapatkan dari user itu dikarenakan jaringan user lama dalam merespon paket yang dikirim dari *user attack* ataupun frame nya yang rendah, sehingga harus mengulangi lagi penggunaan tool kepada user yang lain. Tahapan ke Hasil *cracking*, menampilkan *password*. WPA2-PSK dari proses penyerangan terhadap *user* dengan memecahkan kode enkripsi yang telah di dapat dari *user*. Tahapan Ketujuh Menarik kesimpulan, untuk memutuskan sebuah kesimpulan yang bisa kita terapkan pada saat proses penyerangan oleh *user attack* terhadap keamanan WPA2-PSK pada jaringan WiFi dilihat dari sisi (*success/fail*). Menulis laporan dari proses-proses penyerangan yang telah dilakukan untuk mendapatkan *password* keamanan WPAPSK pada jaringan WiFi.³ Setelah berhasil masuk maka *Hacker* memakai paket data internet tanpa sepengetahuan pemilik WiFi.

Pada tahapan pencurian paket data internet di atas, diketahui bahwa korban pemilik WiFi mengalami kerugian paket data, untuk provider internet Telkomsel misalnya, untuk pemakaian paket data internet 14 *Gigabytes* nilai nominalnya Rp.100.000. Pada paket IndiHome 10Mbps, batas pemakaian didapatkan adalah 300 GB. Namun, jika pemakaian internet mencapai 300GB, kecepatannya akan diturunkan menjadi 75% atau 7.5Mbps. Paket IndiHome 20Mbps tentu menawarkan kuota FUP yang lebih besar. FUP IndiHome 20Mbps 2021 yang pertama, yaitu 500GB, dengan kecepatan yang diturunkan menjadi 75%. Jika orang yang mengalami pencurian data internet tidak sadar maka dengan sendirinya dia akan kehilangan akses internet karena paket data internetnya telah dipakai habis. Kemudian, saat pemakaian sudah menyentuh 400GB maka kecepatan internet kembali diturunkan menjadi 40% atau sekitar 4Mbps.

Penelitian ini memfokuskan penelitian bukan pada proses pencurian data internet, namun penelitian mengangkat isu hukum atau rumusan masalah apakah paket data internet dapat dijadikan sebagai alat bukti pada pengadilan?

2. Metode Penelitian

Tulisan ini memakai jenis penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif atau penelitian hukum kepustakaan (*Library research*).⁴ Penelitian hukum normatif mengkaji hukum yang dikonsepsikan sebagai norma atau kaidah yang berlaku. Norma hukum yang berlaku itu berupa norma hukum positif tertulis bentukan lembaga perundang-undangan (undang-undang dasar, kodifikasi, undang-undang, peraturan pemerintah, dan sebagainya).⁵ Tipe penelitian yang dipakai dalam penulisan ini bersifat Deskriptif Analitis.⁶ Dengan alasan bahwa hasil yang didapatkan dari studi

³ *Ibid*

⁴ Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, cet.4, Raja Grafindo Persada, Jakarta, 1995, hlm 13-14.

⁵ Abdulkadir Muhammad, *Hukum dan Penelitian Hukum*, cet.1, Citra Aditya Bakti, Bandung, 2004, hlm 52.

⁶ Roni Hanitjo Soemitro, *Metodologi Penelitian Hukum dan Yurimetri*, Ghalia Indonesia, Jakarta, 1980 hlm, 12.

kepuustakaan selanjutnya dianalisis dan dibahas dengan menggunakan alur pembahasan secara sistematis didalam beberapa bab. Kemudian hasil analisis pembahasan tersebut dideskripsikan untuk mempermudah penarikan kesimpulan dan pengajuan saran.

Adapun yang menjadi sumber bahan hukum yang diperlukan dalam penelitian ini yaitu bahan hukum sekunder berdasarkan studi pustaka/studi literatur (*library research*).

Sumber bahan hukum tersebut diklasifikasikan antara lain:

Bahan hukum primer diperoleh melalui studi kepuustakaan atau penelitian studi kepuustakaan. Bahan hukum ini ialah yang mempunyai otoritas. Bahan hukum ini terdiri atas peraturan perundang-undangan sesuai hierarki, yaitu :

- 1) Kitab Undang-undang Hukum Pidana
- 2) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- 3) Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Bahan hukum sekunder meliputi bahan-bahan yang mendukung bahan hukum primer seperti buku teks, artikel, dalam berbagai majalah ilmiah atau jurnal hasil penelitian dibidang hukum, makalah-makalah yang disampaikan dalam berbagai bentuk pertemuan seperti diskusi, seminar, dan lain-lain.

Bahan hukum tersier diperoleh dari majalah-majalah hukum, brosur, internet, kamus, dan faktor-faktor hukum yang terjadi dalam praktek. Sedangkan sesuai dengan sifat penelitian maka analisis dan teknik pengumpulan bahan hukum yang dipakai adalah Analisis Kualitatif yaitu dengan cara mempelajari dan memahami data yang ada selanjutnya dianalisis dengan metode induktif dan deduktif sehingga dapat ditarik kesimpulan dalam rangka menjawab permasalahan dalam penulisan ini.⁷

3. Hasil Dan Pembahasan

Pembaharuan hukum adalah salah satu solusi untuk mengejar ketertinggalan hukum atas teknologi yang terus berkembang. Usaha Pembaharuan hukum di Indonesia yang sudah dimulai sejak lahirnya UUD 1945 tidak dapat dilepaskan pula dari landasan dan sekaligus tujuan yang ingin dicapai seperti telah pula dari landasan dan sekaligus tujuan yang ingin dicapai seperti yang telah dirumuskan juga dalam Pembukaan UUD 1945. Tujuan yang telah digariskan dalam pembukaan UUD 1945 itu secara singkat ialah “melindungi segenap bangsa Indonesia dan untuk memajukan kesejahteraan umum berdasarkan Pancasila”. Inilah garis kebijakan umum yang menjadi landasan dan sekaligus tujuan politik hukum di Indonesia. Ini pula yang menjadi landasan dan tujuan dari setiap usaha pembaharuan hukum, termasuk pembaharuan di bidang hukum pidana dan kebijakan penanggulangan kejahatan di Indonesia.⁸

⁷ Soerjono Soekamto, *Pengantar Penelitian Hukum*, Rajawali Press, Jakarta, 2003, Hlm 15.

⁸ Barda Nawawi Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, GENTA, Yogyakarta, 2010. hlm 1-2

Wetboek Van Strafrecht Nederland dengan adanya putusan Mahkamah Agung Nederland (HR tanggal 23 Mei 1921, W 10726, NJ 1921. 564) yang memutuskan "energi listrik" sebagai bagian dari "barang" seperti dimaksudkan dalam pasal 310 N. W.v.S. (Pasal 362 KUHP) dalam kasus "arrest listrik" tahun 1921, Hoge Raad memberlakukan pasal 310 N.W.v.S. (Pasal 362 KUHP) yang secara jelas menunjuk istilah "barang" (*goed*) di dalam rumusan kaidahnya. Istilah "barang" (*goed*) sebenarnya merupakan unsur kaidah yang sangat umum sehingga memiliki ruang lingkup yang begitu luas. Pemahaman terhadap istilah "barang" pada saat itu hanya sebatas, barang berwujud" saja. Sehingga ketika Hoge Raad memberikan putusannya tanggal 23 Mei 1921, makna dan pemahaman terhadap istilah "barang" bertambah bukan hanya berupa "barang berwujud" tetapi juga "barang tidak berwujud" (dalam kasus ini 'arus listrik') yang masih termasuk di dalam makna barang sebagaimana dimaksudkan dalam Pasal 310 N.W.v.S.⁹

Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwa yang bersalah melakukannya. Pasal 184 ayat (1) menyatakan Alat bukti yang sah ialah : a. keterangan saksi; b. keterangan ahli; c. surat; d. petunjuk; e. keterangan terdakwa.¹⁰ *Positif Wettelijks theorie* atau Sistem Pembuktian Berdasarkan Undang-Undang Positif merupakan Sistem ini ditempatkan berhadapan dengan sistem pembuktian conviction in time, karena sistem ini menganut ajaran bahwa bersalah tidaknya terdakwa didasarkan kepada ada tiadanya alat-alat bukti sah menurut undang-undang yang dapat dipakai membuktikan kesalahan terdakwa. Sistem positif wettelijk sangat mengabaikan dan sama sekali tidak mempertimbangkan keyakinan hakim. *Negative Wettelijk* atau Sistem Pembuktian Berdasarkan Undang-Undang Secara Negatif adalah dimana hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwa yang bersalah melakukannya. Jika dilihat dari konteks Pasal 183 KUHP, maka dapat diambil kesimpulan bahwa KUHP di Indonesia memiliki sistem pembuktian yang bersifat *negative wettelijk*.¹¹

Majelis hakim harus yakin dengan uraian Jaksa tentang apakah bisa menggambarkan kerugian yang timbul akibat pencurian paket data internet oleh *hecker*, untuk itu perlu adanya penggambaran dari pihak jaksa dengan mengemukakan dalil dengan menghadirkan pendapat-pendapat hukum dari ahli yang dapat menyakinkan hakim. Pada Pasal 44 Undang-Undang Nomor 11

⁹ Hwian Christianto, Batasan dan Perkembangan Penafsiran Ekstensif dalam Hukum Pidana, Jurnal Pamator, Volume 3, Nomor 2, Oktober 2010

¹⁰ M. Yahya Harahap, Pembahasan Permasalahan dan Penerapan KUHP Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali: Edisi Kedua, (Sinar Grafika), Jakarta, 2006, hlm 319.

¹¹ Ali Imron, Muhamad Iqbal, Hukum Pembuktian, UNPAM PRESS, 2019. hlm1 31

Tahun 2008 tentang Informasi dan Transaksi Elektronik Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

- a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan
- b. 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 5

- (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.

Pada penjelasan Pasal 5 dan Pasal 44 Undang-Undang Nomor 11 Tahun 2008, diketahui bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah, penetapan informasi, dokumen dan hasil cetak dokumen merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Hasil cetak dokumen elektronik yang dimaksud adalah hasil cetakan yang kemudian diperiksa oleh ahli digital forensik atau lembaga yang berwenang mengeluarkan surat keterangan bahwa dokumen elektronik tersebut adalah benar.

Bagaimana dengan paket data internet, pada setiap computer yang terkoneksi ke Internet diberi alamat yang berbeda. Alamat ini supaya seragam seluruh dunia maka pemberian alamat *IP address* diseluruh dunia diberikan oleh badan internasional *Internet Assigned Number Authority (IANA)*, dimana IANA hanya memberikan *IP address Network ID* nya saja sedangkan host ID diatur oleh pemilik IP address tersebut. rekam jejak yang berisikan informasi atau data historis mengenai hasil penelusuran seseorang yang disebut dengan jejak digital. Dalam penelitian sebelumnya yang dilakukan oleh Wang mengenai pelacakan

jejak digital rujukan utama artikel ilmiah yang ditemukan dari platform jejaring sosial yang diikuti oleh bookmark atau URL di ketik di mesin pencarian umum atau browser. Jejak digital dapat dengan mudah dilacak dari berbagai sistem pencarian atau penelusuran sumber informasi secara online. Media sosial memiliki peran yang penting dalam penelusuran informasi yang terintegrasi dengan akun dan situs ataupun platform google. Layanan dan kebijakan mengenai akses privasi situs penelusuran seperti di YouTube tercantum jelas dalam versi *Term and Condition* pada Google. Layanan berisikan mengenai konektivitas antara situs penelusuran baik melalui browser dan android saling terhubung. Produk yang terintegrasi dengan aplikasi dan situs pihak ketiga, seperti iklan dan Google Maps tersemat dan saling terintegrasi satu sama lain. Hasil penelusuran yang telah dilakukan oleh seseorang di browser maupun media yang terintegrasi memiliki sistem pengumpulan informasi atau catatan database oleh Google. Kebijakan sistem informasi tersebut menjelaskan bahwa sistem mengumpulkan informasi yang sering dikunjungi atau diakses seperti iklan yang paling sering dicari, orang yang paling sering berkomunikasi dengan anda, ataupun video YouTube yang disukai oleh anda telah dikelola dan dikumpulkan oleh Google.¹²

Jejak digital ini akan kelihatan di provider untuk pengambilan paket data yang diakses oleh provider, kemudian hasil digital forensik yang dilakukan diterbitkan yang menjelaskan IP *address* yang mengakses dan berapa banyak paket data yang dicuri. Dari Putusan *Hoge Raad* dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

4. Kesimpulan

Jadi pulsa data internet merupakan barang bukti elektronik, dan dapat dibawa ke hadapan pengadilan untuk dinilai, hal ini sesuai dengan Pasal 44 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, perluasan barang bukti ini juga terlihat dalam kasus "arrest listrik" tahun 1921, Hoge Raad memberlakukan pasal 310 N.W.v.S. (pasal 362 KUHP) yang secara jelas menunjuk istilah "barang" (*goed*) di dalam rumusan kaidahnya.

Ucapan terima Kasih (*Acknowledgments*)

Lembaga Penelitian dan Pengabdian Masyarakat

Fakultas Hukum Universitas Pattimura

¹² Evi Aprilia Sari, Pengaruh Aktivitas Penelusuran Informasi Terhadap Jejak Digital Di Youtube Bagi Generasi Millennial, BIBLIOTIKA : Jurnal Kajian Perpustakaan dan Informasi Volume 4 Nomor 1, 2020

Daftar Referensi

Jurnal

Baihaqi, Yeni Yanti, Zulfan, Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi, *Serambi Engineering*, Volume III, No.1, Januari 2018

Evi Aprilia Sari, Pengaruh Aktivitas Penelusuran Informasi Terhadap Jejak Digital Di Youtube Bagi Generasi Millennial, *BIBLIOTIKA : Jurnal Kajian Perpustakaan dan Informasi* Volume 4 Nomor 1, 2020

Erwin Ubwarin, Kebijakan Formulasi Hukum Pidana Dalam Penanggulangan Tindak Pidana Perjudian Melalui Internet (Internet Gambling), *Jurnal Sasi*, Volume 23. Nomor 1. Bulan Januari - Juni 2017

Hwian Christianto, Batasan dan Perkembangan Penafsiran Ekstensif dalam Hukum Pidana, *Jurnal Pamator*, Volume 3, Nomor 2, Oktober 2010

Buku

Abdulkadir Muhammad, *Kajian Hukum Pidana Ekonomi*, PT. Citra Aditya Bakti, Bandung, 2011

Abdulkadir Muhammad, *Hukum dan Penelitian Hukum*, cet.1, Citra Aditya Bakti, Bandung, 2004

Ali Imron, Muhamad Iqbal, *Hukum Pembuktian*, UNPAM PRESS, 2019.

Barda Nawawi Arief, *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, GENTA, Yogyakarta, 2010.

M. Yahya Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali: Edisi Kedua*, (Sinar Grafika), Jakarta, 2006.

Roni Hanitjo Soemitro, *Metodologi Penelitian Hukum dan Yurimetri*, Ghalia Indonesia, Jakarta, 1980

Soerjono Soekanto, *Pengantar Penelitian Hukum*, Rajawali Press, Jakarta, 2003

Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, cet.4, Raja Grafindo Persada, Jakarta, 1995