Criminal Liability of Eavesdroppers On Public Wi-Fi Networks [Pertanggungjawaban Pidana Pelaku Kejahatan Penyadapan Pada *Public Wi-Fi Networks*]

Mudiatul Farikha[1]); M. Tanzil Multazam[2)]

[1)] Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia
[2)] Program Studi Ilmu Hukum, Universitas Muhammadiyah Sidoarjo, Indonesia
mudiatulfarikha99@gmail.com, tanzilmultazam@umsida.ac.id

Abstract. *Technology is developing rapidly resulting in a borderless world as well as being a means of unlawful action that is troubling on the security side. With the internet as many as 202.6 million people in Indonesia, making them vulnerable as targets for cybercrime users carried out in various modes, one of which is wiretapping on public wifi networks. This study was conducted to find out how the process and legal consequences for someone who does wiretapping on a public wifi network. This research uses a normative research method with a statutory approach. The analysis of legal materials is carried out qualitatively. The establishment of Law no. 11 of 2008 concerning ITE which is expected to be able to handle criminal acts of information technology crimes that are troubling to the public and there are definite guarantees and the use of cyberspace so that in the future it can be developed to the fullest.*

Keyword - *accountability; Tapping; public wifi.*

Abstrak. *Teknologi berkembang pesat mengakibatkan dunia menjadi tanpa batas sekaligus dapat menjadi sarana perbuatan melawan hukum yang merisaukan pada sisi keamanan. Dengan pengguna internet sebanyak 202,6 juta orang di Indonesia menjadikan rentan sebagai sasaran kejahatan dunia maya yang dilakukan dengan berbagai modus, salah satunya yaitu penyadapan pada public wifi networks. Penelitian ini dilakukan untuk mengetahui bagaimana proses dan akibat hukum bagi seseorang yang melakukan penyadapan pada public wifi networks. Penelitian ini menggunakan metode penelitian normatif dengan pendekatan perundang undangan. Analisis bahan hukum dilakukan secara kualitatif. Terbentuknya Undang Undang No.11 Tahun 2008 tentang ITE yang diharap mampu menangani tindak pidana kejahatan teknologi infromasi yang merisaukan masyarakat dan adanya jaminan yang pasti serta pemanfaatan dunia maya kedepannya menjadi lebih dikembangkan secara maksimal.*

Kata Kunci - *pertanggungjawaban; penyadapan; public wifi.*

I. PENDAHULUAN

Maraknya layanan public Wi-Fi Networks yang terdapat pada hampir semua kawasan keramaian mempermudah masyarakat untuk mendapatkan koneksi internet dengan menggunakan bantuan dari kecanggihan teknologi informasi yang ada pada saat ini. Teknologi informasi telah berkembang pesat yang mengakibatkan dunia menjadi tanpa batas dan sekaligus dapat menjadi sarana dalam perbuatan melawan hukum. Munculnya teknologi informasi adalah suatu kepentingan yang tidak bisa dihilangkan demi mendukung pembangunan nasional. Akan tetapi pada sisi keamanan dalam menggunakan fasilitas internet terdapat ancaman yang sangat merisaukan. Keamanan yang terdapat pada jaringan internet harus lebih diawasi, sebab jaringan internet yang sifatnya universal memiliki kelemahan dan rawan terhadap bermacam-macam bentuk kejahatan. Penggunaan internet yang bertujuan tidak baik oleh faktor dari manusia itu sendiri yang menjadikan pengguna internet lainnya merasa cemas. Jika dilihat dalam dunia maya manusia inilah yang dinamakan sebagai cracker atau hacker. [1]

Dilansir dari Kompas.com pada bulan September tahun 2021, terdapat laporan terkait adanya peretasan sistem jaringan yang dimiliki oleh Badan Intelijen Negara (BIN) termasuk juga meretas akun sepuluh kementerian dan lembaga negara Indonesia. Insikt Group yang merupakan lembaga peneliti keamanan internet mendeteksi adanya malware dengan jenis PlugX yang dijalankan oleh group Mustang Panda sebagai server pengendali perintah. Server tersebut telah berinteraksi dengan beberapa localhost yang ada pada jaringan internal yang dimiliki oleh pemerintah Indonesia dengan kemungkinan telah terinfeksi. [2] Dengan pengguna internet sebanyak 202,6 juta orang di Indonesia menjadikan negara ini rentan sebagai sasaran kejahatan dunia maya yang dapat dilakukan dengan berbagai modus seperti pishing, carding, virus malware atau software, pembobolan kartu kredit, dll. [3]

Copyright © Universitas Muhammadiyah Sidoarjo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Sebuah penelitian yang dilakukan pada tahun 2015 oleh Ruchir Bhatnagar dan Vineet Kumar Birla yang berjudul "*Security in Wireless Network"* bahwa organisasi yang menggunakan jaringan nirkabel protocol standart *IEEE 802.11* belum sepenuhnya aman dan masih sangat rentan terhadap serangan yang menyebabkan data maupun informasi bisa disadap maupun di hacking. [4]

Berdasarkan hasil penelitian terdahulu menjadikan salah satu tumpuan penulis didalam menjalankan penelitian sehingga mampu untuk mempebanyak teori dan sudut pandang yang dipakai untuk meninjau penelitian yang dilakukan. Penelitian yang pertama, Maisarah pada tahun 2020, "Pencurian Internet Wi-Fi Menurut Pasal 30 Undang-Undang Nomor 19 Tahun 2016 Tentang ITE". Pada penelitian ini menggunakan metode penelitian kualitatif, yang membahas mengenai modus melakukan pencurian jaringan Wi-Fi di Kuala Bansa Aceh pada daerah Syiah Kuala. Serta mengulas bagaimana sudut pandang hukum islam mengenai pencurian pada internet Wi-Fi. Pada kesimpulannya seseorang yang telah mencuri internet wifi bisa dijatuhi pidana dengan Pasal 30 ayat (1), (2), dan (3) *jo* Pasal 46 ayat (1), (2) dan (3) Undang-Undang No 19 Tahun 2016 Tentang ITE. Penelitian kedua, Rizkyani pada tahun 2020, "Analisis Keamanan Jaringan Pada Fasilitas Internet Wifi oleh Serangan Packet Snifing yang terjadi pada Kantor Koran Seruya". Metode penelitian pada penelitian ini yaitu kualitatif yaitu berupa riset dengan menggunakan analisis dan bersifat penjelasan. Pada penelitian ini membahas mengenai bagaimana cara untuk alisis jaringan wireles yang aman pada serangan paket snifing yang terjadi pada kantor koran seruya. Dan dalam penelitian ini terdapat sebuah kesimpulan bahwa protect terhadap jaringan yang terdapat pada kantor koran seruya harus lebih ditingkatkan yang terbukti pada wifi yang tidak menggunakan keamanan atau open (terbuka). Sehingga rentan terhadap kejahatan teknologi.

Namun, terdapat perbedaan yang membedakan antara penelitian yang dilakukan penulis dengan beberapa penelian diatas yaitu terdapat pada metode penelitiannya, dimana pada beberapa penelitian diatas menggunakan metode penelitian kualitatif, sementara itu peneliti disini menggunakan metode penelitian normative dengan pendekatan undang-undang.

Berdasarkan uraian tersebut maka penelitian ini bertujuan untuk mengetahui bagaimana proses dan akibat hukum bagi seseorang yang melakukan penyadapan pada public wifi networks. Pada penyusunan penelian ini diharap mampu memberikan manfaat yang bisa digunakan sebagai wawasan dan pemahaman terhadap akademisi hukum, mahasiswa, serta kewaspadaan kepada masyarakat luas khususnya pengguna teknologi informasi dalam menggunakan layanan wifi public agar lebih berhati-hati.

II. METODE

Jenis penelitian yang dilakukan pada penelitian ini yaitu menggunakan metode penelitian jenis normatif dengan menggunakan pendekatan perundang undangan (*statute approach*), dimana dalam pendekatan ini akan dilakukan dengan menggunakan cara mengulas undang undang serta regulasi yang ada hubungannya dengan isu hukum yang sedang diatasi. [5] Dengan bahan hukum primer yang meliputi :

a. Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
b. Undang Undang Nomor 36 Tahun 1999 tentang Telekomunikasi
c. Undang Undang Nomor 19 Tahun 2019 tentang Komisi Pemberantasan Korupsi

Sedangkan bahan hukum sekunder diperoleh dari hasil yang digunakan untuk menunjang data primer yang meliputi buku, jurnal, yang bertautan dengan apa yang akan diteliti. Analisis bahan hukum dalam penelitian ini dakukan secara kualitatif kemudian dikaji menggunakan logika deduktif dengan menghubungkan teori teori dari studi kepustakaan yang selanjutnya akan dapat ditarik kesimpulan yang akan digunakan untuk menjawab rumusan masalah dalam penelitian ini.

III. HASIL DAN PEMBAHASAN

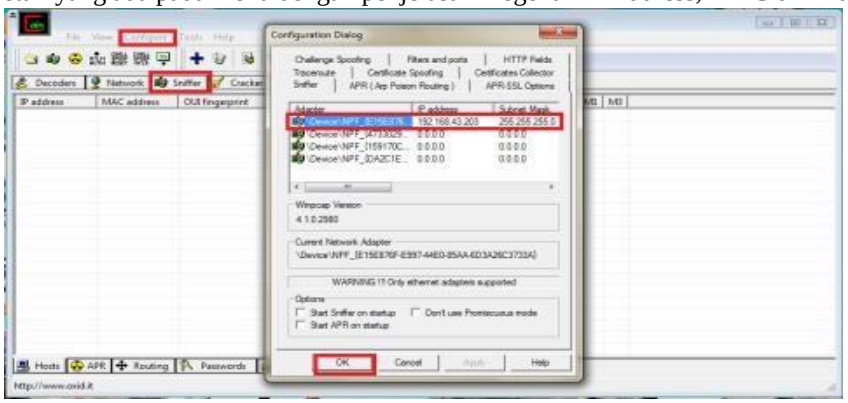
A. Proses Penyadapan Pada Public Wi-Fi Networks.

Jaringan internet Wi-Fi layaknya tempat yang mempunyai fungsi untuk menyambungkan satu perangkat pada perangkat lainnya dengan otomatis jika orang lain mampu menerobos atau menyusup pada suatu sistem keamanan wifi dan mampu memasuki jaringan tersebut, yang akan terjadi adalah seseorang tersebut akan bebas dan leluasa untuk membuka semua perangkat elektronik milik orang lain yaitu pada handphone, komputer dan laptop orang lain yang telah terkoneksi pada wifi dalam jaringan yang sama. Maka dari itu pelaku bisa dengan mudah memiliki kendali pada perangkat milik orang lain, juga mampu untuk mengambil data penting dan data milik pribadi tanpa sepengetahuan orang lain seperti foto, gambar, video, akun mobile banking, dan banyak akun penting lainnya. [6]

Penyadapan pada suatu jaringan dibagi dalam dua kategori yaitu penyadapan pasif dan penyadapan aktif. penyadapan passive yaitu penyadapan yang dilakukan dengan cara tidak mengubah paket data apapun dari suatu jaringan, sementara pada penyadapan aktif, dilakukan dengan cara mengubah paket data pada suatu jaringan. Penyadapan dilakukan dengan menggunakan tool tambahan, salah satunya dengan menggunakan aplikasi Cain and Abel. Langkah-langkah untuk menggunakan aplikasi Cain And Abel: [7]

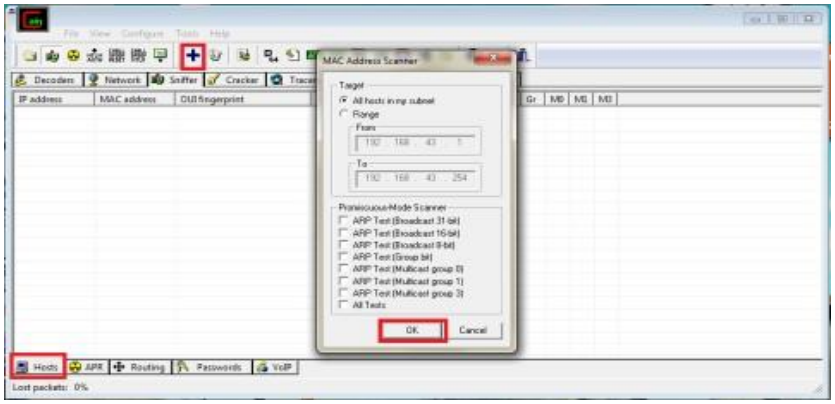
Copyright © Universitas Muhammadiyah Sidoarjo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

1. Download aplikasi Cain and Abel, kemudian install
2. Tekan tombol Configure – kemudian akan terlihat configure dialog yang isinya mengenai bebeapa menu configuration – tekan tab Sniffer – kemudian akan muncul penjelasan mengenai Adapter, IP Address dll – tekan pada deretan yang ada pada menu dengan penjelasan megenai IP Address, MAC dll – lalu tekan OK



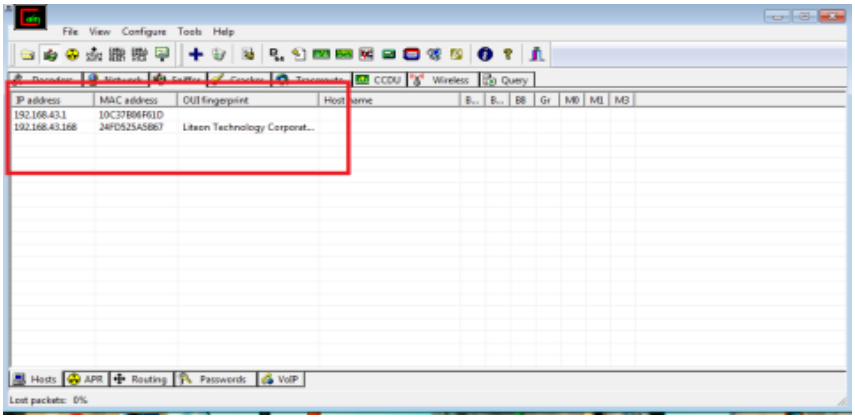
Gambar 1 Petunjuk Button

3. Klik table host, kemudian aktifkan Cain dengan mengklik tombol Start. Tekan tombol (Add to list) untuk mencari MAC Adress kemudian



Gambar 2 scan mac address

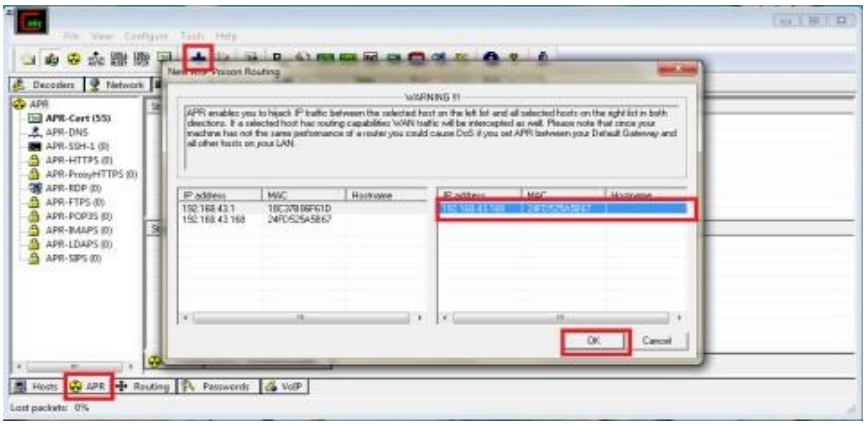
4. Klik APR



Gambar 3 petunjuk APR Button

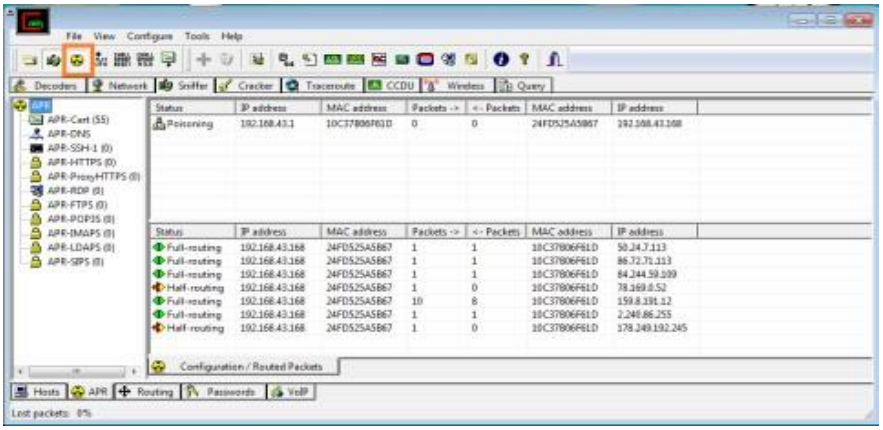
5. Kemudian akan terlihat tulisan dialog New ARP Poison Routing. Lalu tekan IP Address pada perangkat yang menjadi sasaran yang berada pada bagian kiri lalu tekan IP Address perangkat gateway yang ada dalam bagain sebelah kanan. Kemudian tekan OK

Copyright © Universitas Muhammadiyah Sidoarjo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.



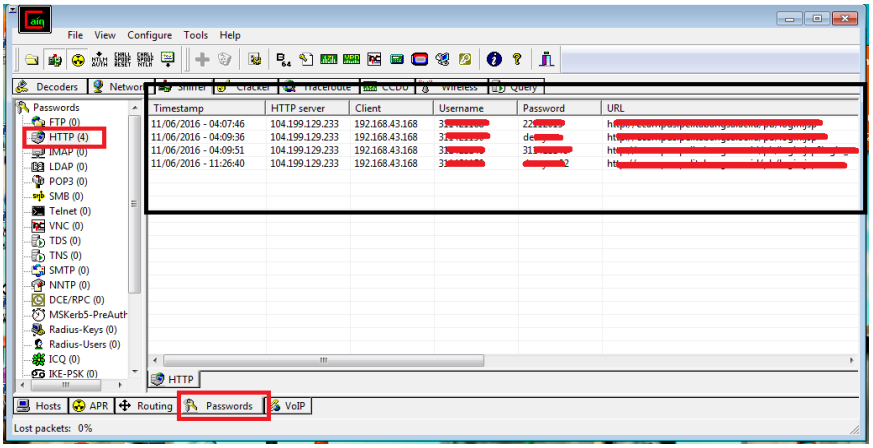
Gambar 4 petunjuk IP Address

6. Kemudian masuk pada list tekan tombol start ARP, lalu tunngu agar lalu lintas paket data yang terambil oleh aplikasi. Semua aktifitas korban akan terekam saat korban melakukan login password yang dimilikinya.



Gambar 5 proses routing

7. Untuk melihat password, klik tabel Password kemudian pilih di tabel sebelah kiri jenis password yang terekam oleh cain



Gambar 6 Hasil Sniffing

Jika melihat pada proses penyadapan tersebut merupakan suatu tindakan melawan hukum, dimana hal tersebut merupakan suatu tindakan penyadapan yang memantau lalu lintas data pada jaringan internet menggunakan cara yaitu membaca data yang ada di internet dengan bantuan alat tambahan yaitu sniffer software atau hardware, juga digunakan untuk memperoleh informasi yaitu data rahasia dan juga passsword. Suatu tindakan apabila mengancam dan membuat rugi kepentingan umum maka dalam hukum pidana perbuatan tersebut adalah suatu perbuatan yang melawan hukum. Unsur unsur yang ada pada perbuatan melawan hukum didalam hukum pidana yaitu perbuatan tersebut secara tegas dinyatakan sebagai perbuatan yang melanggar undang undang, dan juga perbuatan tersebut

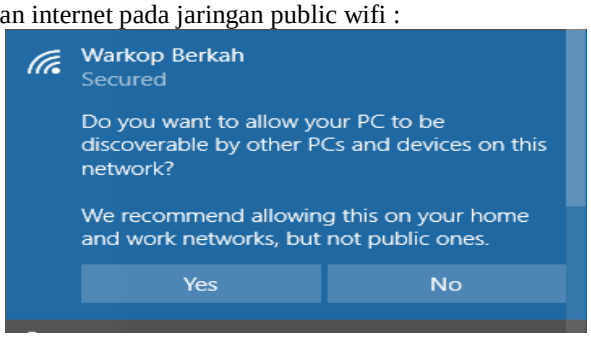
Copyright © Universitas Muhammadiyah Sidoarjo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

dilaksanakan tanpa memiliki kewenangan serta kekuasaan dan juga suatu tindakan yang tidak mematuhi asas asas umum yang terdapat pada lapangan hukum. [8]

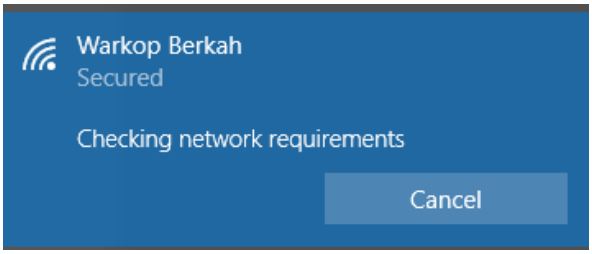
Pada dasarnya setiap penyedia atau pemilik layanan public wifi dapat mengontrol dengan akses penuh dari aktivitas dengan berbagai macam pada jaringan tersebut, apabila pengguna layanan tersebut mengakses internet maka semua yang diakses akan terekam pada wifi. Karena ketika pengguna mengakses internet tentunya membutuhkan data dari internet, arus transaksi data dari internet tadi tentunya harus bisa dilihat juga oleh wifi. Sangat dimungkinkan bagi penyedia layanan wfi untuk dapat melihat riwayat pencarian internet dari orang yang menggunakan layanan internet wifi. Namun sebelum hal itu dilakukan, dalam sebuah perangkat terdapat router yang mempunyai pengaturan dan fungsi yang berbeda. Salah satunya justru memerlukan beberapa alat atau aplikasi tambahan seperti proxy server, firmware, maupun wireShark yang mampu digunakan untuk mencatat paket data yang ada dan juga memilah juga menunjukkan data. [9]

Pada dasarnya sebuah jaringan internet yang bersifat publik merupakan sebuah tempat yang tidak cukup aman untuk dipakai. Terdapat berbagai macam kelemahan yang akan bisa digunakan oleh seseorang atau pelaku yang berniat jahat. Pada banyaknya resiko ini juga tidak sedikit mendatangkan ketakutan. Salah satu diantaranya yaitu rasa cemas yang timbul bahwa pengelola atau pemilik layanan wifi publik yang dapat melihat apa saja yang telah diakses oleh pengguna layanan wifi padahal hal tersebut merupakan sebuah privasi.

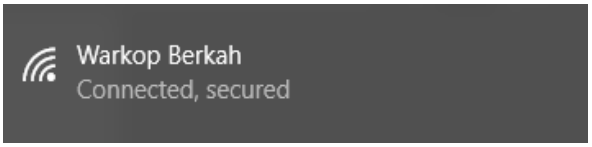
Setiap orang yang mengelola layanan public wifi tidak hanya bisa mengakses aktivitas pengguna jaringan wifi saja, namun juga dapat mengakses data pribadi, kemudian pada pemilik layanan public wifi yang sejauh mana dia dikatakan menyadap karena walaupun tanpa adanya suatu niatan untuk menyadap, telah memiliki akses kontrol atas perangkat elektronik pengguna layanan wifi milik orang lain, karena pada saat seseorang akan menghubungkan perangkat elektronik pada jaringan public wifi akan muncul kata *agreement* **(tabel 7)** yang berisikan keterangan mengenai persetujuan apakah bersedia untuk perangkat komputernya diakses oleh penyedia layanan public wifi dengan pilihan yaitu “yes atau no” untuk dapat terhubung ke dalam jaringan wifi tersebut **(tabel 9).** Apabila seseorang memilih “yes” berarti telah menyetujui jika perangkat komputernya dapat diakses orang lain, apabila memilih “no” maka tidak dapat diakses oleh orang lain. Kemudian pada hal ini apabila seseorang menyetujui dengan memilih “yes” maka hal tersebut menjadikan penyedia layanan public wifi tidak dapat dihukum dikarenakan adanya persetujuan dari pengguna yang telah memilih “yes” pada saat menghubungkan pada jaringan public wifi.
Langkah-langkah menghubungkan internet pada jaringan public wifi :



Gambar 7 Persetujuan login wifi



Gambar 8 Menghubungkan Jaringan



Gambar 9 Jairngan Terhubung

B. Akibat Hukum Bagi Pelaku Penyadapan Pada Public Wi-Fi Networks

Pada konsep penyadapan di Indonesia, dapat dilihat pada beberapa peraturan perundang undangan yang berlaku. Peraturan perundang undangan tersebut diantaranya yaitu Undang Undang Telekomunikasi, Undang

Copyright © Universitas Muhammadiyah Sidoarjo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Undang Informasi dan Transaksi Elektrnonik, Undang Undang Komisi Pemberantasan Korupsi. Terdapat penjelasan mengenai penyedia jasa layanan telekomunikasi pada upaya penegakkan hukum juga dalam permintaan aparat penegakkan hukum yang berwenang, pada hal tersebut yang dimaksud yaitu Kepala Kepolisian, Jaksa Agung, ataupun penyidik tindak pidana tertentu, hal tersebut terdapat dalam Pasal 42 dan Pasal 43 Undang Undang Telekomunikasi **(tabel 1.1**). Kemudian jika dilihat dalam Undang Undang Informasi dan Transaksi Elektronik yang telah memberi suatu hak yang bersifat legal kepada aparat penegak hukum dalam melaksanakan atau dimintanya untuk melakukan tidakan penyadapan. Pada Pasal 31 yang menjelaskan mengenai tindakan penyadapan yang menurut undang undang diperbolehkan yaitu penyadapan tersebut harus dilaksanakan dalam upaya penegakan hukum oleh permintaan aparat yang berwenang **(tabel 1.1).** Pada hal pemberantasan tindak pidana korupsi pada Pasal 12 Undang Undang Komisi Pemberantasan Korupsi, salah satu wewenang KPK adalah melaksanakan tindakan menyadap dan merekam pembicaraan **(tabel 1.1)**. Meskipun legalitas KPK untuk melakukan penyadapan telah diatur, dalam Undang Undang Komisi Pemberantasan Korupsi sendiri tidak mengatur atau mendefinisikan secara jelas terkait definisi dari penyadapan maupun batasan batasan kewenangan penyadapan tersebut. [9]

Tabel 1.1 Perbandingan Penyadapan Terkait Subyek Dan Wewenang

Klasifikasi	**Undang-Undang ITE**	**Undang-Undang Telekomunikasi**	**Undang-Undang KPK**
Subyek	Setiap orang yang dengan sengaja melakukan penyadapan (Perbuatan melawan Hukum) (Pasal 31 ayat 1)	Jaksa Agung, Kepala Kepolisian (Pasal 42)	Anggota KPK
Wewenang	Ketentuan Pasal 31 ayat 1 tidak berlaku bagi setiap aparat dalam rangka penegakkan hukum.	Penyedia layanan jasa telekomunikasi dapat merekam informasi yang dikirim atau diterima (Pasal 43)	Penyadapan telepon dan perekaman pembicaraan
Batasan	Hanya berlaku bagi aparat (Kepolisian, Kejaksaan, Institusi yang berwenang)	• Hanya untuk keperluan proses peradilan • Untuk tindak pidana tertentu • Atas permintaan tertulis Jaksa Agung dan Kepala Kepolisian	• Hanya untuk kepentingan peradilan dalam pemberantasan tindak pidana korupsi (Pasal 12D ayat 1) • Dilaksanakan setelah mendapatkan izin tertulis dari Dewan Pengawas (Pasal 12B ayat 1)

Terdapat tiga unsur dalam akibat hukum yaitu yang pertama, lahirnya, berubahnya, atau lenyapnya suatu keadaan hukum. Kedua, lahirnya, berubahnya atau lenyapnya suatu hubungan hukum. Ketiga, lahirnya sanksi apabila dilakukan tindakan yang melawan hukum. Akibat hukum dari suatu penyadapan pada public wifi networks adalah berupa lahirnya sanksi apabila dilakukan tindakan yang melawan hukum. Penyadapan sebagaimana yang telah diuraikan diatas menunjukkan bahwa telah terjadi suatu tindakan melawan hukum yang dilakukan dengan cara menyadap sebuah public wifi networks. Pelaku yang melakukan penyadapan atau masuk secara paksa pada sistem yang telah diberikan pengamanan (password) wifi yang dimiliki orang lain secara tidak sah dengan menggunakan berbagai macam cara.

Sebagaimana telah diuraikan pada unsur penyadapan yang memenuhi ketentuan Pasal 31 ayat (1) Undang Undang Nomor 11 Tahun 2008 tentang ITE diantaranya yaitu : [10]

1.) Setiap orang
2.) Dengan sengaja
3.) Tanpa hak atau melawan hukum atau *(wederrechtelijk)*
4.) Melakukan intersepsi atau penyadapan
5.) Atas informasi elektronik dan/atau dokumen elektronik dalam satu komputer maupun sistem elektronik tertetu milik orang lain

Unsur pertama, terkait dengan kata setiap orang, menunjukkan siapa saja orang yang apabila orang tersebut memenuhi semua unsur dari tindakan penyadapan secara sengaja dan tanpa hak, jadi seseorang itu dapat disebut sebagai pelaku penyadapan ataupun disebut sniffer. Unsur kedua, terkait dengan kata dengan sengaja, penyadapan

Copyright © Universitas Muhammadiyah Sidoarjo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

data pribadi pengguna internet yang dilakukan seseorang yang biasa disebut dengan sniffer merupakan suatu kesengajaan dari seseorang yang tidak mempunyai hak dengan maksud untuk membuat untung dirinya sendiri. Pada kata dengan maksud atau met het oogmerk itu dapat diartikan dengan tujuan oleh pelaku untuk membuat untung dirinya sendiri maupun orang lain yang dilakukan dengan cara melawan hukum atau *wederrechtelijk*. Pada unsur ketiga, terkait dengan membuat untung dirinya sendiri maupun orang lain yang dilakukan dengan cara melawan hukum memiliki penafsiran yaitu sebuah keuntungan yang didapatkan lalu dalam mendapatkan untung tersebut dilakukan secara bertentangan dari keseharusan dalam lingkungan masyarakat. Faisal Thayib mengklasifikasikan suatu tindakan menyadap pada Pasal 31 Undang Undang ITE merupakan *computer related crime* dalam bentuk *illegal interception.* [11]

Unsur keempat, terkait dengan melakukan tindakan penyadapan. Kegiatan yang dilakukan dengan cara mendengar, membelokkan, merubah, merekam juga menyatat suatu transmisi elektronik maupun dokumen elektronik yang bukan bersifat publik, yang dilakukan dengan bantuan jaringan kabel komunikasi ataupun jaringan nirkabel, yaitu radio frekuensi ataupun pancaran elektromagnetis. Penyadapan data pribadi pengguna internet yang dilakukan pada public wifi networks pelaku atau sniffer melakukan penyadapan dengan cara membelokkan transmisi informasi yang bersifat elektronik maupun dokumen yang bersifat elektronik. Unsur kelima, terkait dengan informasi elektronik maupun dokumen elektronik dalam satu komputer maupun perangkat elektronik yang dimiliki oleh orang lain, merupakan satu ataupun gabungan dari data elektronik, tetapi tidak terbatas pada gambar, tulisan, foto, suara, surat elektonik, maupun kode, symbol yang sudah diolah yang dapat mempunyai arti yang hanya mampu dipahami oleh orang terntentu yang paham akan teknologi. [12]

Umumnya pelaku penyadapan atau sniffer melakukan penyadapan untuk memperoleh data pribadi pengguna internet seperti username dan password berupa kode PIN *(personal identification number)* pengguna internet yang kemudian untuk seterusnya username dan password tersebut digunakan untuk mengakses masuk akun pribadi pengguna internet dalam 58 suatu situs tertentu dalam internet. Username dan password tersebut merupakan suatu bentuk dari informasi yang bersifat elektronik maupun dokumen yang bersifat elektronik dimana username beserta password berbentuk suatu tulisan terdiri dari angka, huruf ataupun kode akses yang sudah diubah dan hanya orang tertentu yang dapat memahaminya.

Jika dilihat pada unsur-unsur tersebut, bahwa tindakan penyadapan yang telah dilakukan oleh pelaku tersebut dapat memenuhi unsur subjektif dan objektif, seperti yang telah dijelaskan pada Pasal 31 ayat (1) Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Maka dari itu Pasal tersebut bisa diterapkan pada tindak pidana penyadapan penyadapan pad public wifi networs. Ketentuan hukum yang mengatur tentang penyadapan secara khusus ada dalam Undang Undang Nomor 11 Tahun 2008 tentang ITE. [13] Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 Ayat (1) atau Ayat (2) Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, akan dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.800.000.000,00- (delapan ratus juta rupiah). [14]

Penjelasan mengenai penyadapan juga terdapat dalam Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Penyadapan yang dimaksudkan yaitu suatu tindakan yang dilakukan dengan memasang suatu alat tambahan maupun perangkat yang ada dalam jaringan telekomunikasi dengan bertujuan untuk memperoleh sebuah informasi secara tidak sah. Pada hakikatnya sebuah infromasi milik seseorang merupakan suatu hak yang bersifat pribadi yang wajib dilindungi, maka dari itu penyadapan itu tidak diperbolehkan. Siapapun yang tidak mematuhi aturan tersebut dapat dijatuhi pidana dengan penjara paling lama 15 (lima belas) tahun. Perbuatan menyadp merupakan perbuatan yang melanggar hukum, dimana orang yang telah melakukan hal tersebut atau pelaku bisa dijerat dengan sanksi pidana dapat berupa penjara maupun denda. Pihak yang telah dirugikan akibat perbuatan penyadapan atau intersepsi yang tidak sesuai dengan aturan Undang Undang yang berlaku bisa melaporkan pada instansi yang berwenang yaitu kepolisian.

VII. KESIMPULAN

Proses penyadapan pada public wifi networks dilakukan menggunakan perangkat elektronik dengan cara mendownload software untuk menerobos sistem keamanan dengan tujuan untuk mendapatkan informasi maupun data rahasia, hal tersebut tersebut merupakan suatu tindakan melawan hukum. Kemudian pada pemilik layanan public wifi yang sejauh mana dia dikatakan menyadap karena walaupun tanpa adanya suatu niatan untuk menyadap, telah memiliki akses kontrol atas perangkat elektronik pengguna layanan wifi milik orang lain. Karena pada saat menghubungkan perangkat komputer pada jaringan public wifi akan muncul kata *agreement* yang berisikan keterangan mengenai persetujuan apakah bersedia perangkat komputernya diakses oleh penyedia layanan wifi public dengan pilihan “yes atau no”. Apabila seseorang memilih “yes” maka menjadikan penyedia layanan public wifi tidak dapat dihukum dikarenakan adanya persetujuan dari pengguna yang telah memilih “yes” pada saat menghubungkan perangkat komputer pada jaringan public wifi. Pelaku penyadapan pada public wifi networks dapat dipidana dengan Pasal 31 ayat (1) Undang Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Hal tersebut merupakan akibat hukum dari lahirnya sanksi apabila dilakukan tindakan melawan hukum. Pengecualian dilakukan terhadap ketntuan larangan penyadapan atau intersepsi itu adalah apabila hal tersebut

Copyright © Universitas Muhammadiyah Sidoarjo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

dilakukan dalam rangka penegakkan hukum dan atas permintaan kepolisian, kejaksaan maupun institusi lainnya yang kewenangannya ditetapkan berdasarkan Undang Undang, seperti Komisi Pemberantasan Korupsi.

VIII. UCAPAN TERIMAKASIH

Terimakasih kepada kedua Orang Tua dan kakak saya yang tak henti berdo'a serta memberikan dukungan moril dan materil agar penelitian ini berjalan lancar. Tak lupa juga terimakasih kepada teman teman kelas hukum 8A1 yang telah memberikan semangat pada saat penelitian ini berlangsung.

REFERENSI

[1] I. G. A. S. K. Singgi, "Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime)," *Jurnal Konstruksi Hukum* , vol. 1, no. 2, pp. 334-339, 2020.

[2] "Kompas.com," [Online]. Available: https://tekno.kompas.com/read/2021/09/11/20045197/jaringan-10-kementerian-dan-lembaga-negara-indonesia-diduga-diretas-hacker?page=all. [Diakses 13 Maret 2022].

[3] "Liputan6.com," [Online]. Available: https://www.liputan6.com/tekno/read/4683148/menkominfo-pengguna-internet-di-indonesia-capai-2026-juta-orang-per-januari-2021. [Diakses 21 November 2021].

[4] R. Bhatnagar, "Wi-Fi Security: A Literature Review of Security in Wireless Networks," *International Journal of Research in Enginering and Tehnology*, vol. 3, no. 5, pp. 23-30, 2015.

[5] K. Benuf, "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia," *Jurnal Ilmu Hukum*, vol. 3, no. 2, pp. 145-160, 2019.

[6] M.Syuib, "Tindak Pidana Pencurian Jaringan Wifi Menurut Pasal 30 Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik," *Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial*, vol. 6, no. 1, p. 51, 2021.

[7] Susanto, "Analisis Sniffing Password Menggunakan Aplikasi Cain Dan Abel Pada Jaringan Wifi Universitas Semarang," *Jurnal Transformatika*, vol. 16, no. 1, p. 67, 2018.

[8] I. Sari, "Perbuatan Melawan Hukum (PMH) dalam Hukum Pidana dan Hukum Perdata," *Jurnal Ilmiah Hukum Dirgantara*, vol. 11, no. 1, pp. 53-70, 2020.

[9] R. K. Kagi, "Desain Dan Implementasi Pada Wifi Pustikom Free Access Di Pusat Teknologi Informasi Dan Komunikasi Universitas Negeri Jakarta Menggunakan Mikrotik Dan Wireshark Untuk Analisis Terhadap Serangan Packet Sniffing Dan Netcut," *Jurnal Pendidikan Teknik Informatika dan Komputer*, vol. 4, no. 2, pp. 37-40, 2020.

[10] Sekarsari, "Legalitas Alat Bukti Elektronik Hasil Penyadapan Dalam Rencana Penjebakan Sebagai Upaya Penegakan Hukum," vol. 1, no. 2, p. 705, 2019.

[11] A. M. Rohmy, "UU ITE Dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi," *Jurnal Dakwah dan Komunikasi Islam*, vol. 7, no. 2, p. 309, 2021.

[12] Lisnawati, "Mengurai Undang Undang No.11 Tahun 2008 Tentang ITE dalam Dimensi Pembangunan Cyber Law," *Jurnal Yustika*, vol. 5, no. 2, p. 26, 2009.

[13] C. Y. Serfani, "Buku Pintar Bisnis Online dan Transaksi Elektronik," Jakarta, Gramedia Pustaka Utama, 2012, p. 99.

[14] H. Christianto, "Tindakan Penyadapan Ditinjau Dari Perspektif Hukum Pidana," *Jurnal Hukum Prioris*, vol. 5, no. 2, p. 89, 2015.

[15] I. M. A. Wiraputra, "Sanksi Hukum terhadap Pelaku Penyadapan Telepon Pintar atau Smartphone Melalui Aplikasi Android Modifikasi Ilegal yang Diinstal oleh Korban," *Jurnal Konstruksi Hukum*, vol. 3, no. 2, pp. 450-454, 2022.

Copyright © Universitas Muhammadiyah Sidoarjo. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.