UNIVERSITAS
MUHAMMADIYAH
SIDOARJO

UMSIDA
DARI SINI PENCERAHAN BERSEMI

Pertanggungjawaban Pidana Pelaku Kejahatan Penyadapan Pada Public Wi-Fi Networks

Oleh:

Nama Mahasiswa : Mudiatul Farikha

Nama Dosen Pembimbing : M. Tanzil Multazam

Progam Studi Hukum

Universitas Muhammadiyah Sidoarjo

Agustus, 2022

Pendahuluan

Maraknya layanan public Wi-Fi Networks yang terdapat pada hampir semua kawasan keramaian mempermudah masyarakat untuk mendapatkan koneksi internet dengan mudah. Akan tetapi dalam kemudahan tersebut terdapat ancaman yang sangat merisaukan dalam sisi keamanan.

Dilansir dari Kompas.com pada September 2021, sistem jaringan milik sepuluh kementerian dan lembaga negara Indonesia, termasuk milik Badan Intelejen Negara (BIN) dilaporkan telah diretas. Terdeteksi adanya server penggendali perintah milik group Mustang Panda yang menjalankan malware berjenis PlugX. Server tersebut berkomunikasi dengan beberapa host yang kemungkinan telah terinfeksi di dalam jaringan internal milik pemerintah Indonesia.

Dalam Undang - Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diharapkan mampu menanggulangi tindak pidana teknologi informasi yang semakin meresahkan masyarakat, serta menjamin kepastian dan pemanfaatan cyberspace agar dapat berkembang secara optimal.

Rumusan Masalah

1. Bagaimana proses penyadapan pada public wifi networks ?
2. Apa akibat hukum bagi pelaku penyadapan pada public networks ?

Metode

Jenis Penelitian

Metode Normatif

Pendekatan

Pendekatan Perundang - Undangan

Analisis Bahan Hukum

Analisis deduktif

Bahan Hukum

- Primer
  - Undang - Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
  - Undang - Undang Nomor 36 Tahun 1999 tentang Telekomunikasi
  - Undang - Undang Nomor 19 Tahun 2019 tentang Komisi Pemberantasan Korupsi
- Sekunder

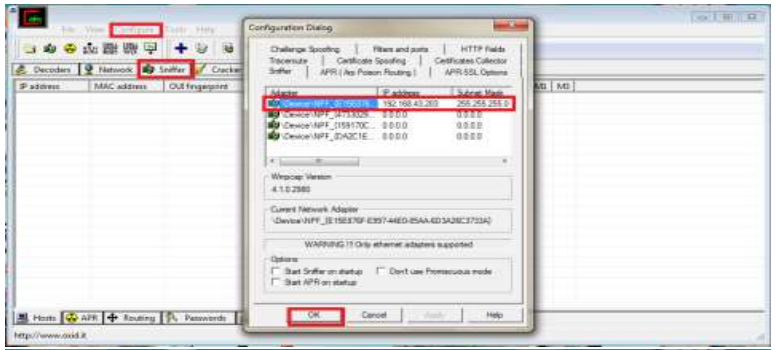
  Bahan sekunder yang digunakan ialah buku, serta jurnal ilmiah yang berkaitan dengan permasalahan yang akan diteliti.

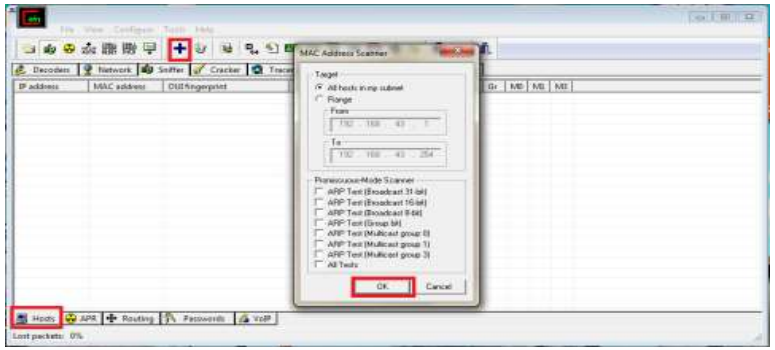
Pembahasan

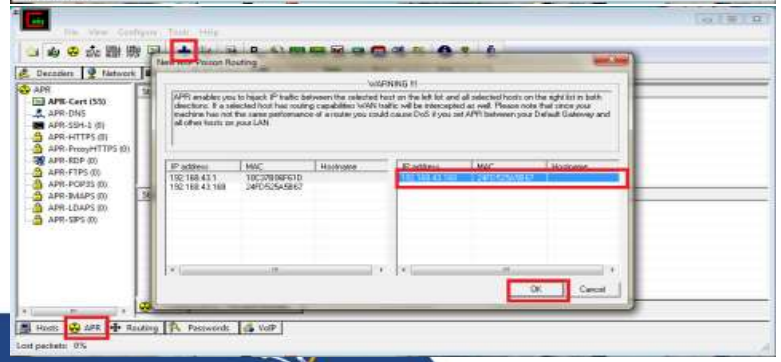
A. Proses Penyadapan Pada Public Wi-Fi Networks

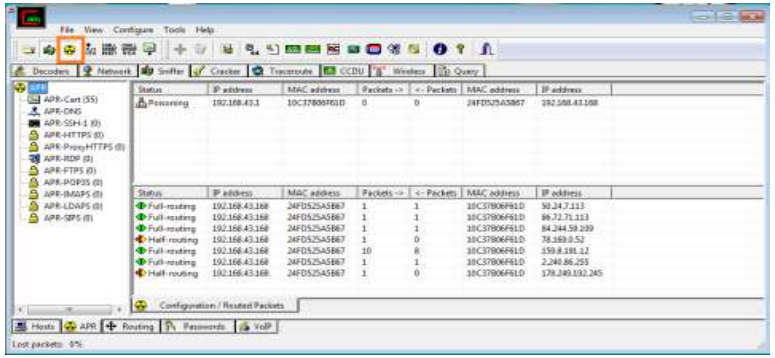
Penyadapan pada suatu jaringan dibagi dalam dua kategori yaitu penyadapan pasif dan penyadapan aktif. penyadapan passive yaitu penyadapan yang dilakukan dengan cara tidak mengubah paket data apapun dari suatu jaringan, sementara pada penyadapan aktif, dilakukan dengan cara mengubah paket data pada suatu jaringan.

Proses Penyadapan menggunakan software CainAndAbel









- Setiap orang yang mengelola layanan wifi publik tidak hanya bisa mengakses aktivitas pengguna jaringan wifi saja, namun juga dapat mengakses data pribadi pengguna akan tetapi untuk melakukan hal tersebut membutuhkan bantuan dari apikasi tambahan. Dalam konteks pemilik wifi publik yang dapat mengakses data pribadi dengan bantuan aplikasi tambahan dari pengguna jaringan wifi publik. Walaupun tanpa adanya suatu niatan untuk menyadap, namun pemilik wifi tersebut telah memenuhi unsur penyadapan yaitu telah sengaja untuk mengakses data tersebut dan melihatnya. Hal tersebut dapat dikatakan telah melakukan suatu tindakan penyadapan,

Pembahasan

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

Terdapat tiga unsur dalam akibat hukum:
Lahirnya, berubahnya, atau lenyapnya suatu keadaan hukum.
Lahirnya, berubahnya atau lenyapnya suatu hubungan hukum.
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. Pelaku yang melakukan penyadapan atau masuk secara paksa pada sistem yang telah diberikan pengamanan wifi yang dimiliki orang lain secara tidak sah dengan menggunakan berbagai macam cara.

Pembahasan

Unsur penyadapan pada Pasal 31 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang ITE:
Setiap orang
Dengan sengaja
Tanpa hak atau melawan hukum
Melakukan intersepsi atau penyadapan
Atas informasi elektronik dan/atau dokumen elektronik dalam satu komputer maupun sistem elektronik tertetu milik orang lain

Tindakan penyadapan yang telah dilakukan oleh pelaku tersebut dapat memenuhi unsur 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 pada public wifi networks.

Ketentuan hukum yang mengatur tentang penyadapan secara khusus ada dalam Undang Undang Nomor 11 Tahun 2008 tentang ITE. Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 Ayat (1) Undang Undang Nomor 11 Tahun 2008 Tentang ITE dapat dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.800.000.000,00-

Hasil

1. Proses penyadapan pada public wifi networks dilakukan menggunakan bantuan perangkat seperti laptop maupun handphone dengan cara memasang aplikasi tambahan untuk dapat menerobos sistem keamanan dengan tujuan memperoleh username dan password jaringan untuk dapat mengakses perangkat pengguna layanan public wifi. Penyedia layanan public wifi walaupun tanpa adanya niatan untuk menyadap, namun untuk dapat mengakses data tersebut harus menggunakan aplikasi tambahan, maka apabila pemilik wifi tersebut telah sengaja untuk mengakses data tersebut dan melihatnya. Hal tersebut dapat dikatakan sebagai tindakan penyadapan.
2. 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. Pelaku harus mempertanggungjawabkan tindakannya karena telah memenuhi unsur dari penyadapan itu sendiri. Pengecualian dilakukan terhadap ketentuan larangan penyadapan apabila hal tersebut dilakukan dalam rangka penegakkan hukum dan atas permintaan kepolisian, kejaksaan maupun institusi lainnya yang kewenangannya ditetapkan berdasarkan Undang Undang, seperti Komisi Pemberantasan Korupsi.

Temuan Penting Penelitian

1. Proses penyadapan pada public wifi networks dapat dilakukan dengan memasang aplikasi tambahan, seperti yang telah dijelaskan dalam penelitian ini yaitu dengan menggunakan aplikasi CainAndAbel.
2. Penyedia layanan public wifi networks mempunyai akses penuh dalam jaringannya. Sehingga mereka dapat dengan mudah untuk mengetahui apa saja yang ditelusuri oleh pengguna layanan wifi tersebut. Namun untuk dapat mengaksesnya penyedia layanan wifi harus masuk terlebih dahulu dalam aplikasi tertentu, maka dalam hal tersebut dilakukan dengan kesengajaan. Maka perbuatan itu dapat dikatakan sebagai penyadapan
3. Penyadapan memiliki pengecualian terhadap ketentuan larangan penyadapan apabila hal tersebut dilakukan dalam rangka penegakkan hukum dan atas permintaan kepolisian, kejaksaan maupun institusi lainnya yang kewenangannya ditetapkan berdasarkan Undang Undang, seperti Komisi Pemberantasan Korupsi.

Manfaat Penelitian

1. Manfaat Teoritis

   Penelitian ini diharapkan mampu menambahkan bahan pustaka yang membehas mengenai kejahatan dunia maya seperti kejahatan penyadapan pada public wifi networks.

2. Manfaat Praktis

   Hasil penelitian ini diharapkan mampu digunakan sebagai wawasan dan pemahaman terhadap akademisi hukum, mahasiswa, serta kewaspadaan kepada masyarakat luas, khususnya pengguna teknologi informasi dalam menggunakan layanan public wifi agar lebih berhati-hati


UMSIDA
DARI SINI PENCERAHAN BERSEMI