BAB III

HASIL PENELITIAN DAN PEMBAHASAN

A. Pembuktian Tindak Pidana Akses Ilegal terhadap Komputer

1. Posisi Kasus

a. Perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 sebagaimana diatur dan diancam pidana dalam Pasal 50 *jo* Pasal 22 huruf b Undang-undang No. 36 Tahun 1999 tentang Telekomunikasi; atau

b. Perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 sebagaimana diatur dan diancam pidana dalam Pasal 46 ayat (1) *jo* Pasal 30 ayat (1) Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; atau

c. Perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 sebagaimana diatur dan diancam pidana dalam Pasak 46 ayat (2) *jo* Pasal 30 ayat (2) Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; atau

d. Perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 sebagaimana diatur dan diancam pidana dalam Pasal 46 ayat (3) *jo* Pasal 30 ayat (3); atau

e. Perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 sebagaimana diatur dan diancam pidana dalam Pasal 48 ayat (1) *jo*

Pasal 32 ayat (1) Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Lima dakwaan di atas merupakan dakwaan yang bersifat alternatif, artinya dari lima dakwaan yang ada hanya satu pasal saja yang akan diteruskan menjadi tuntutan. Hal ini kemungkinan disebabkan adanya kendala dalam pembuktian.

2. Dakwaan Penuntut Umum

Pertama,

Terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada hari dan tanggal yang sudah tidak dapat diingat di pertengahan tahun 2012 sampai dengan tanggal 8 Januari 2013 sekira jam 22.45 WIB atau setidak-tidaknya pada waktu lain dalam tahun 2012 sampai dengan bulan Januari 2013 bertempat di CV Surya Infotama, Jalan Letjen Suprapto No. 169 Kebon Sari Kabupaten Jember Jawa Timur atau setidak-tidaknya pada suatu tempat yang masih termasuk dalam daerah hukum Pengadilan Negeri Jember, melakukan perbuatan tanpa hak, tidak sah, atau manipulasi akses ke jasa telekomunikasi. Perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dilakukan dengan cara sebagai berikut:

a. Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada waktu dan tempat sebagaimana tersebut di atas selaku operator billing Warnet Surya Com milik CV Surya Infotama, telah merentas server my.Techscape.co.id dan membuat account secara illegal pada webshoting www.jatirejanetwork.com dengan menggunakan

seperangkat komputer billing Warnet Surya Com milik CV Surya Infotama, sedangkan untuk software menggunakan tools berupa scit khusus yang berbasiskan bahasa pemrograman PHP.

b. Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dengan menggunakan nickname MJL007 terhadap website www.jatirejanetwork.com dengan IP Address 210.247.249.58 bergerak dibidang pelayanan domain hosting milik dan dikelola saksi Eman Sulaiman bin Enjen yang dibeli dari saksi D.A. Giovanno Setyawardhana. Selanjutnya terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menemukan sebuah celah keamanan website www.jatirejanetwork.com, kemudian melakukan SQL Injection dan berhasil menanamkan sebuah backdoor berupa tools (software) yang berbasiskan bahasa pemrograman PHP yang bernama wso.php (web sell by orb) kemudian disimpan dalam harddisk komputer billing Warna Surya Com terletak di drive D: Master pada folder: 001-MASTERSOFTWARE\009-TOOL\root.

c. Bahwa selanjutnya terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan keamanan server website yang sama IP Address-nya dengan techscape.co.id milik CV Techscape dengan IP Address 202.155.61.121 dan menemukan celah keamanan, sehingga dapat disimpulkan bahwa server techscape.co.id memiliki celah keamanan yang sama. Kemudian terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan reverse ip lookup terhadap website

dimaksud dengan menggunakan tool on line (web based) www.yougetsignal.com berhasil mendapatkan informasi bahwa website yang dimaksud memiliki IP Address 202.155.61.121, lalu terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan dan menemukan satu website yang merupakan webhosting yaitu www.techscape.co.id, selanjutnya melakukan pencarian terhadap direktori yang didalamnya terdapat konfigurasi WHMCS (Web Host Manager Complete Solution) yaitu aplikasi yang biasa digunakan untuk web web hosting management, dan ditemukan direktori dimaksud adalah my.techscape.co.id.

d. Bahwa sekitar bulan November 2012 terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan akses terhadap website www.jatirejanetwork.com yang telah berhasil diterobos dengan teknik SQL Injection dan telah ditanamkan backdoor wso, selanjutnya menjalankan command linux: cat/home/tech/www/my/configuration.php melalui backdoor wso yang telah ditanam sebelumnya dan berhasil mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape yaitu username: “tech_whmcs dan password: “y16=V=1J&mL(“, kemudian terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menjalankan tool WHMKiller dari domain website www.jatirejanetwork.com untuk mendapatkan username dan password dari domain manager setiap domain name yang ada di server web hosting dari WHM control panel

antara lain username: “root” dan password: “b4p4kg4nt3ngTIGA” dengan port nomor: 2086, selanjutnya melakukan akses ke server techscape.co.id dengan IP Address: 202.151.61.121 port: 2086 melalui brower Mozila Firefox, setelah mendapatkan akses ke WHM Control Panel mengisi username: “root” dan password: “b4p4kg4nt3ngTIGA” kemudian menanamkan tool backdoor wso.php dengan cara melakukan uploading tool backdoor wso.php pada server techscape.co.id pada tanggal 16 November 2012 jam 04.58:31 WIB. Agar backdoor tersebut tidak diketahui oleh admin techscape.co.id maka terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan perubahan nama (rename) terhadap tool dimaksud menjadi “domain.php” ditempatkan di sub direktori my.techscape.co.id maka terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dapat mengakses server techscape.co.id kapanpun melalui url: my.techscape.co.id/feeds/domain.php dengan password: “yayan123”.

e. Bahwa pada tanggal 8 Januari 2013 sekitar 20.00 WIB terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan akses ke website www.enom.com selaku domain registrar techscape.co.id dan selanjutnya melakukan login ke akun techscape menggunakan username: techscape dan password: “tcs800puri”. Setelah berhasil melakukan login ke akun techscape di domain registrar enom (eNom, Inc, USA) tersebut mendapatkan informasi DSN Server dari domain presidensby.info, yaitu:

1. Sahi78679.eart.orderboxdns.com;
2. Sahi78679.mars.orderbox-dns.com;
3. Sahi78679.venus.orderbox-dns.com; dan
4. Sahi78679.mercury.orderbox-dns.com

Selanjutnya diubah menjadi:

1. Id1.jatirejanetwork.com; dan
2. Id2jatirejanetwork.com.

Kemudian terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada jam 22.45 WIB melakukan pembuatan (create) akun domain presdensby.info di server pihak perusahaan webhosting jatirejahost.com dan menempatkan sebuah file HTML "Jember Hacker Team" di server jatirejahost.com, sehingga ketika para user internet tidak dapat mengakses konten website www.presidensby.info yang sebenarnya, akan tetapi konten yang terakses oleh para user adalah tampilan file HTML "Jember Hacker Team".

f. Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 merentas server my.techscape.co.id milik CV Techscape. Dan membuat account secara ilegal oada webhosting website www.jatirejanetwork.com milik dan dikelola saksi Eman Sulaiman bin Enjen dengan menggunakan tools khusus berupa scrift khusus yang berbasiskan bahasa pemrograman PHP dengan modus redireting DNS sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 berinteraksi dengan sistem milik my.techscape.co.id dan

www.jatirejanetwork.com yang mana keduanya merupakan penyedia hosting dan bertindak sebagai Internet Service Provider (ISP) yang merupakan penyelenggara multimedia yang termasuk di dalam bagian dari Penyelenggaraan Jasa Telekomunikasi dan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan hal tersebut tanpa seijin dari CV Techscape dan saksi Eman Sulaiman bin Enjen.

g. Bahwa selanjutnya saksi Grawas Sugiharto sebagai anggota subdit IT dan Cyber Crime Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Mabes Polri melakukan penyelidikan atas illegal DNS rederection terhadap website www.presidensby.info dan hasil penyelidikan menemukan alamat tempat terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan perbuatannya tersebut di atas yaitu Warnet CV Surya Infotama, Jl. Letjen Suprapto No. 169 Kebon Sari Jember Jawa Timur. Kemudian saksi Grawa Sugiharto menyamar sebagai pengguna warnet dan melakukan wawancara dengan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada tanggal 25 Januari 2013 sekitar jam 18.00 WIB dan mengakui bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 memiliki akun nickname MJL007 di website forum hacker jember-hacker.org. Selain itu saksi Grawas Sugiharto melihat langsung di komputer billing Warnet Surya Com tersimpan file database perusahaan hosting techscape.co.id dalam format file notepad (.txt). Sekitar jam 23.00 WIB saksi Grawas Sugiharto bersama Tim Penyidik Subdit IT dan Cyber Crime

Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Mabes Polri melakukan penangkapan terhadap Wildan Yani Ashari alias Yayan alias MJL007.

ATAU

Kedua,

Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada hari dan tanggal yang sudah tidak dapat diingat di pertengahan tahun 2012 sampai dengan tanggal 8 Januari 2013 sekira jam 22.45 WIB atau setidak-tidaknya pada waktu lain dalam tahun 2012 sampai dengan bulan Januari 2013 bertempat di CV Surya Infotama, Jl. Letjen Suprapto No. 169 Kebon Sari Kabupaten Jember Jawa Timur atau setidak-tidaknya pada suatu tempat yang masih termasuk dalam daerah hukum Pengadilan Negeri Jember, dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun. Perbuatan ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dilakukan dengan cara sebagai berikut:

a. Bahwa ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada waktu dan tempat sebagaimana tersebut di atas selaku operator *billing* Warnet Surya Com milik CV Surya Infotama, telah mengakses komputer dan/atau sistem elektronik www.jatirejanetwork.com dan server my.Techscape.co.id dengan menggunakan seperangkat komputer *billing* Warnet Surya Com milik CV Surya Infotama,

sedangkan untuk software menggunakan tools berupa scrit khusus yang berbasiskan bahasa pemrograman PHP.

b. Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dengan menggunakan nickname MJL007 terhadap website www.jatirejanetwork.com dengan *ip address* 210.247.249.58 bergerak dibidang pelayanan domain hosting milik dan dikelola saksi Eman Sulaiman bin Enjen yang dibeli dari saksi D.A. Giovanno Setyawardhana. Selanjutnya terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menemukan sebuah celah keamanan *website* www.jatirejanetwork.com kemudian melakukan SQL *Injection* dan berhasil menanamkan sebuah *backdoor* berupa *tools* (*software*) yang berbasiskan bahasa pemrograman PHP yang bernama wso.php (*web sell by orb*) kemudian disimpan dalam *harddisk* komputer *billing* Warnet Surya Com terletak di drive D: master pada folder: 001-MASTER SOFWARE\009-TOOL\root.

c. Bahwa selanjutnya terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan keamanan server website yang sama ip address-nya dengan techscape.co.id milik CV Techscape dengan *ip address* 202.155.61.121 dan menemukan celah keamanan, sehingga dapat disimpulkan bahwa server techscape.co.id memiliki celah keamanan yang sama. Kemudian terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan reverse ip lookup terhadap website dimaksud dengan menggunakan tool on line (web based)

www.yougetsignal.com berhasil mendapatkan informasi bahwa website dimaksud memiliki *ip address* 202.155.61.121, lalu terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan dan menemukan satu website yang merupakan webhosting yaitu www.techscape.co.id. Selanjutnya melakukan pencarian terhadap direktori yang didalamnya terdapat konfigurasi WHMCS (Web Host Manager Complete Solution) yaitu aplikasi yang biasa digunakan untuk webhosting management, dan ditemukan direktori dimaksud adalah my.techscape.co.id.

d. Bahwa sekitar bulan November 2012 terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan akses terhadap website www.jatirejanetwork.com yang telah berhasil diterobos dengan teknik SQL Injection dan telah ditanamkan backdoor wso, selanjutnya menjalankan command linux: cat/home/tech/www/my/configuration.php melalui backdoor wso yang telah ditanam sebelumnya dan berhasl mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape yaitu username: “tech_whmcs dan password: “y16=V=1J&mL(“, kemudian terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menjalankan tool WHMKiller dari domain website www.jatirejanetwork.com untuk mendapatkan username dan password dari domain manager setiap domain name yang ada di server webhosting dari WHM control panel antara lain username: “root” dan password: “b4p4kg4nt3ngTIGA”

dengan port nomor: 2086, selanjutnya melakukan akses ke server techscape.co.id dengan *ip address*: 202.155.61.121 port: 2086 melalui browser Mozilla Firefox, setelah mendapatkan akses ke WHM Control Panel mengisi username: “root” dan password: “b4p4kg4nt3ngTIGA” kemudian menanamkan tool backdoor wso.php dengan cara melakukan uploading tool backdoor wso.php pada server techscape.co.id pada tanggal 16 November 2012 jam 04:58:31 WIB. Agar backdoor tersebut tidak diketahui oleh admin techscape.co.id maka terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan perubahan nama (rename) terhadap tool dimaksud menjadi “domain.php” ditempatkan di sub direktori my.techscape.co.id/feeds/, sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dapat mengakses server techscape.co.id kapanpun melalui url: mytechscape.co.id/feeds/domain.php dengan password: “yayan123”.

e. Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada tanggal 8 Januari 2008 sekitar jam 20.00 WIB melakukan akses ke website www.enom.com selaku domain registrar techscape menggunakan username: techscape dan password: “tcs800puri” tersebut di atas dan setelah berhasil melakukan login kea kun techscape di domain registrar enom (eNom, Inc, USA) tersebut mendapatkan informasi tentang DNS Sever dari domain presidenby.info, yaitu:

1. Sahi78679.eart.orderboxdns.com;

2. Sahi78679.mars.orderbox-dns.com;
3. Sahi78679.venus.orderbox-dns; dan
4. Sahi78679.mercury.orderbox-dns.com

Selanjutnya diubah menjadi:

1. Id1.jatirejanetwork.com; dan
2. Id2jatirejanetwork.com.

f. Bahwa perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dengan mencari konfigurasi WHMCS (Web Host Manager Complete Solution) dengan mengakses URL www.techscape.co.id dan memilik menu login sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menemukan direktori my.technoscape.co.id (aplikasi membhosting management) dan mengubah tool WHMKiller guna mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape.co.id, menjalankan command Linux: cat/home/tech/www/myconfiguration.php melalui backdoor wso sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 berhasil mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape yaitu username: “techwhmsc” dan password “y16=V=1J&mL(, menjalankan tool WHMKiller sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 mendapatkan database yang berisi sejumlah username dan password dari domain manager yang diserver www.techscape.co.id, melakukan akses ke server techscape.co.id sehingga terdakwa Wildan Yani Ashari alias

Yayan alias MJL007 mendapatkan username dan password dari WHM control panel yaitu “root” dan “b4p4kg4nt3ngTIGA”, mengakses server techscape.co.id dengan ip address: 202.151.61.121 port 2086 melalui broser Mozilla Firefox, melakukan akses ke website www.enom.com selaku pihak domain register techscape.co.id dan selanjutnya melakukan login ke akun techscape dan password “tcs800puri” tanpa seijin pemiliknya yaitu CV Techscape dan mengakses sistem website www.jatirejanetwork.com dan mengganti DNS Presindensby, lalu terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pembuatan (create) akun domain presidenby.info di server pihak perusahaan webhosting jatirejahost.com dan menempatkan sebuah file HTML “Jember Hacker Team” di server jatirejahost.com, sehingga ketika para user internet akan dapat mengakses konten website www.presidenby.info yang sebenarnya, akan tetapi konten yang terakses oleh para user adalah tampilan file HTML “Jember Hacker Team”, hal tersebut tanpa seijin dari pemilik dan pengelolanya yaitu saksi Eman Sulaiman Bin Enjen.

g. Bahwa selanjutnya saksi Grawas Sugiharto sebagai anggota Subdit I dan Cyber Crimer Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Mabes Polri melakukan penyelidikan atas illegal DNS rederection terhadap website www.presidenby.info dan hasil penyelidikan menemukan alamat tempat terdakwa Wildan Yani Ashari alias Yayan alias MJL007 terdakwa Wildan Yani Ashari alias Yayan

alias MJL007 melakukan perbuatannya tersebut di atas yaitu Warnet CV Surya Infotama, Jalan Letjen Suprapto No. 169, Kebon Sari Jember, Jawa Timur. Kemudian saksi Grawas Sugiharto menyamar sebagai pengguna warnet dan melakukan wawancara dengan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada tanggal 25 Januari 2013 sekitar jam 18.00 WIB dan mengakui bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 memiliki akun nickname MJL007 di website forum hacker jember-hacker.org, selain itu saksi Grawas Sugiharto melihat langsung di komputer billing Warnet Surya Com tersimpan file database perusahaan hosting techscape.co.id dalam format file notepad (.txt). Sekitar jam 23.00 WIB saksi Grawas Sugiharto bersama Tim Penyidik Subdit IT dan Cyber Crime Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Mabes Polri melakukan penangkapan terhadap Wildan Yani Ashari alias Yayan alias MJL007.

Perbuatan ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 sebagaimana diatur dan diancam pidana dalam Pasal 46 ayat (1) jo Pasal 30 ayat (1) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

ATAU

Ketiga:

Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada ahri dan tanggal yang sudah tidak dapat diingat di pertengahan tahun

2012 sampai dengan tanggal 08 Januari 2013 sekira jam 22.45 WIB atau setidak-tidaknya pada waktu lain dalam tahun 2012 sampai dengan bulan Januari 2013 bertempat di CV Surya Infotama, Jalan Letjen Suprapto No. 169, Kebon Sari Kab. Jember, Jawa Timur atau setidak-tidaknya pada suatu tempat yang masih termasuk dalam daerah hukum Pengadilan Negeri Jember dengan sengaja dan atanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dan/atau dokumen elektronik. Perbuatan ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dilakukan dengan cara sebagai berikut:

a. Bahwa ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada waktu dan tempat sebagaimana tersebut di atas selaku operator *billing* Warnet Surya Com milik CV Surya Infotama, telah mengakses komputer dan/atau sistem elektronik www.jatirejanetwork.com dan server my.techscape.co.id dengan menggunakan seperangkat komputer *billing* Warnet Surya Com milik CV Surya Infotama, sedangkan untuk software menggunakan tools berupa scrit khusus yang berbasiskan bahasa pemrograman PHP
b. Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dengan menggunakan nickname MJL007 terhadap website www.jatirejanetwork.com dengan *ip address* 210.247.249.58 bergerak dibidang pelayanan domain hosting milik dan dikelola saksi Eman Sulaiman bin Enjen yang dibeli dari saksi D.A. Giovanno Setyawardhana. Selanjutnya terdakwa Wildan Yani Ashari alias Yayan

alias MJL007 menemukan sebuah celah keamanan website www.jatirejanetwork.com, kemudian melakukan SQL Injection dan berhasil menanamkan sebuah backdoor berupa tools (software) yang berbasiskan bahsa pemrograman PHP yang bernama wso.php (web sell by orb) kemudian disimpan dalam harddisk komputer billing Warnet Surya Com terletak di drive D: Master pada folder: 001-MASTER SOFTWARE\009-TOOL\root.

c. Bahwa selanjutnya terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan keamanan server website yang sama ip addres-nya dengan techscape.co.id milik CV Techscape dengan *ip address* 210.247.249.58 dan menemukan celah keamanan, sehingga dapat disimpulkan bahwa server techscape.co.id memiliki celah keamanan yang sama. Kemudian terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan reverse ip lookup terhadap website yang dimaksud dengan menggunakan tool on line (web based) www.yougetsignal.co, berhasil mendapatkan informasi bahwa website dimaksud memiliki *ip address* 210.247.249.58, lalu terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan dan menemukan satu website yang merupakan webhosting yaitu www.techscape.co.id, selanjutnya melakukan pencarian terhadap direktori yang didalamnya terdapat konfigurasi WHMCS (WebHost Manager Complete Solution) yaitu aplikasi yang biasa digunakan

untuk webhosting management, dan ditemukan direktori dimaksud adalah my.techscape.co.id.

d. Bahwa sekitar bulan November 2012 terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan akses terhadap website www.jatirejanetwork.com yang telah berhasil diterobos dengan teknik SQL Injection dan telah ditanamkan backdoor wso, selanjutnya menjalankan command linux: cat/home/tech/www/my/configuration.php melalui backdoor wso yang telah ditanam sebelumnya dan berhasil mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape yaitu username: "tech_whmcs dan password: "y16=V=1J&mL(", kemudian terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menjalankan tool WHMKiller dari domain website www.jatirejanetwork.com untuk mendapatkan username dan password dari domain manager setiap domain name yang ada di server webhosting dari WHM control panel antara lain username: "root" dan password: "b4p4kg4nt3ngTIGA" dengan port nomor: 2086, selanjutnya melakukan akses ke server techscape.co.id dengan ip address: 202.151.61.121 port: 2086 melalui browser Mozilla Firefox, setelah mendapatkan askes ke WHM control panel mengisi username: "root" dan password: "b4p4kg4nt3ngTIGA" kemudian menanamkan tool backdoor wso.php dengan cara melakukan uploading tool backdoor wso.php pada server techscape.co.id pada tanggal 16 November 2012 ja, 04.58:31 WIB.

Agar backdoor tersebut tidak diketahui oleh admin techscape.co.id maka terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan perubahan nama (rename) terhadap tool dimaksud menjadi "domain.php" ditempatkan di sub direktori my.techscape.co.id/feeds/, sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dapat mengakses server techscape.co.id kapanpun melalui url: my.techscape.co.id/feeds/domaind.php dengan password: "yayan123"

e. Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada tanggal 08 Januari 2008 sekitar jam 20.00 WIB melakukan akses ke website www.enom.com selaku domain registrar techscape.co.id dan selanjutnya melakukan login keakun techscape menggunakan username: techscape dan password: "tcs800puri" tersebut di atas dengan tujuan untuk mendapatkan informasi tentang DNS Server dari domain presidensmy.info, yaitu

   1. Sahi78679.eart.orderboxdns.com;
   2. Sahi78679.mars.orderbox-dns.com;
   3. Sahi78679.venus.orderbox-dns; dan
   4. Sahi78679.mercury.orderbox-dns.com

f. Bahwa perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dengan mencari konfigurasi WHMCS (Web Host Manager Complete Solution) dengan mengakses URL www.techscape.co.id dan memilik menu login sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menemukan direktori my.technoscape.co.id

(aplikasi membhosting management) dan mengubah tool WHMKiller guna mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape.co.id, menjalankan command Linux: cat/home/tech/www/myconfiguration.php melalui backdoor wso sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 berhasil mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape yaitu username: "techwhmsc" dan password "y16=V=1J&mL(, menjalankan tool WHMKiller sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 mendapatkan database yang berisi sejumlah username dan password dari domain manager yang diserver www.techscape.co.id, melakukan akses ke server techscape.co.id sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 mendapatkan username dan password dari WHM control panel yaitu "root" dan "b4p4kg4nt3ngTIGA", mengakses server techscape.co.id dengan ip address: 202.151.61.121 port 2086 melalui broser Mozilla Firefox, melakukan akses ke website www.enom.com selaku pihak domain register techscape.co.id dan selanjutnya melakukan login ke akun techscape dan password "tcs800puri" tanpa seijin pemiliknya yaitu CV Tecrhscape dengan tujuan untuk mendapatkan informasi tentang DSN Server dari domain presidenby.info dan mengakases website www.jatirejanetwork.com dengan tujuan mengganti DNS presidensby.info tanpa seijin pemilik dan pengelolanya yaitu saksi Eman Sulaiman Bin Enjen menjadi:

1. Id1.jatirejanetwork.com; dan
2. Id2jatirejanetwork.com.

Dan akibat perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada jam 22.45 WIB melakukan pembuatan (create) akun domain presidensby.info di server pihak perusahaan webhosting jatirejahost.com dan menempatkan sebuah file HTML "Jember Hacker Team" di server jatirejahost.com, sehingga ketika para user internet tidak dapat mengakses konten website www.presidensby.info yang sebenarnya, akan tetapi konten yang terakses oleh para user adalah tampilan HTML "Jember Hacker Team."

g. Bahwa selanjutnya saksi Grawas Sugiharto sebagai anggota Subdit I dan Cyber Crimer Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Mabes Polri melakukan penyelidikan atas illegal DNS rederection terhadap website www.presidenby.info dan hasil penyelidikan menemukan alamat tempat terdakwa Wildan Yani Ashari alias Yayan alias MJL007 terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan perbuatannya tersebut di atas yaitu Warnet CV Surya Infotama, Jalan Letjen Suprapto No. 169, Kebon Sari Jember, Jawa Timur. Kemudian saksi Grawas Sugiharto menyamar sebagai pengguna warnet dan melakukan wawancara dengan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada tanggal 25 Januari 2013 sekitar jam 18.00 WIB dan mengakui bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 memiliki akun nickname

MJL007 di website forum hacker jember-hacker.org, selain itu saksi Grawas Sugiharto melihat langsung di komputer billing Warnet Surya Com tersimpan file database perusahaan hosting techscape.co.id dalam format file notepad (.txt). Sekitar jam 23.00 WIB saksi Grawas Sugiharto bersama Tim Penyidik Subdit IT dan Cyber Crime Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Mabes Polri melakukan penangkapan terhadap Wildan Yani Ashari alias Yayan alias MJL007.

Perbuatan ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 sebagaimana diatur dan diancam pidana dalam Pasal 46 ayat (2) jo Pasal 30 ayat (2) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

ATAU

Keempat:

Bahwa ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada hari dan tanggal yang sudah tidak dapat diingat di pertengahan tahun 2012 sampai dengan tanggal 08 Januari 2013 sekira jam 22.45 WIB atau setidak-tidaknya pada waktu lain dalam tahun 2012 sampai dengan bulan Januari 2013 bertempat di CV Surya Infotama, Jalan Letjen Suprapto No. 169, Kebon Sari Kab. Jember, Jawa Timur atau setidak-tidaknya pada suatu tempat yang masih termasuk dalam daerah hukum Pengadilan Negeri Jember dengan sengaja dan atanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dan/atau dokumen

elektronik. Perbuatan ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dilakukan dengan cara sebagai berikut:

a. Bahwa ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada waktu dan tempat sebagaimana tersebut di atas selaku operator *billing* Warnet Surya Com milik CV Surya Infotama, telah mengakses komputer dan/atau sistem elektronik www.jatirejanetwork.com dan server my.techscape.co.id dengan menggunakan seperangkat komputer *billing* Warnet Surya Com milik CV Surya Infotama, sedangkan untuk software menggunakan tools berupa scrit khusus yang berbasiskan bahasa pemrograman PHP
b. Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dengan menggunakan nickname MJL007 terhadap website www.jatirejanetwork.com dengan *ip address* 210.247.249.58 bergerak dibidang pelayanan domain hosting milik dan dikelola saksi Eman Sulaiman bin Enjen yang dibeli dari saksi D.A. Giovanno Setyawardhana. Selanjutnya terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menemukan sebuah celah keamanan website www.jatirejanetwork.com, kemudian melakukan SQL Injection dan berhasil menanamkan sebuah *backdoor* berupa *tools* (*software*) yang berbasiskan bahasa pemrograman PHP yang bernama wso.php (*web sell by orb*) kemudian disimpan dalam harddisk komputer billing Warnet Surya Com terletak di drive D: Master pada folder: 001-MASTER SOFTWARE\009-TOOL\root.

c. Bahwa selanjutnya terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan keamanan server website yang sama ip addres-nya dengan techscape.co.id milik CV Techscape dengan *ip address* 210.247.249.58 dan menemukan celah keamanan, sehingga dapat disimpulkan bahwa server techscape.co.id memiliki celah keamanan yang sama. Kemudian terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan *reverse ip lookup* terhadap website yang dimaksud dengan menggunakan tool on line (*web based*) www.yougetsignal.co, berhasil mendapatkan informasi bahwa website dimaksud memiliki *ip address* 210.247.249.58, lalu terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan dan menemukan satu website yang merupakan webhosting yaitu www.techscape.co.id, selanjutnya melakukan pencarian terhadap direktori yang didalamnya terdapat konfigurasi WHMCS (*WebHost Manager Complete Solution*) yaitu aplikasi yang biasa digunakan untuk webhosting management, dan ditemukan direktori dimaksud adalah my.techscape.co.id.

d. Bahwa sekitar bulan November 2012 terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan akses terhadap website www.jatirejanetwork.com yang telah berhasil diterobos dengan teknik SQL Injection dan telah ditanamkan backdoor wso, selanjutnya menjalankan command linux: cat/home/tech/www/my/configuration.php melalui backdoor wso yang

telah ditanam sebelumnya dan berhasil mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape yaitu username: “tech_whmcs dan password: “y16=V=1J&mL(“, kemudian terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menjalankan tool WHMKiller dari domain website www.jatirejanetwork.com untuk mendapatkan username dan password dari domain manager setiap domain name yang ada di server webhosting dari WHM control panel antara lain username: “root” dan password: “b4p4kg4nt3ngTIGA” dengan port nomor: 2086, selanjutnya melakukan akses ke server techscape.co.id dengan ip address: 202.151.61.121 port: 2086 melalui browser Mozilla Firefox, setelah mendapatkan askes ke WHM control panel mengisi username: “root” dan password: “b4p4kg4nt3ngTIGA” kemudian menanamkan tool backdoor wso.php dengan cara melakukan uploading tool backdoor wso.php pada server techscape.co.id pada tanggal 16 November 2012 ja, 04.58:31 WIB. Agar backdoor tersebut tidak diketahui oleh admin techscape.co.id maka terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan perubahan nama (rename) terhadap tool dimaksud menjadi “domain.php” ditempatkan di sub direktori my.techscape.co.id/feeds/, sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dapat mengakses server techscape.co.id kapanpun melalui url: my.techscape.co.id/feeds/domaind.php dengan password: “yayan123”

e. Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada tanggal 08 Januari 2008 sekitar jam 20.00 WIB melakukan akses ke website www.enom.com selaku domain registrar techscape.co.id dan selanjutnya melakukan login keakun techscape menggunakan username: techscape dan password: “tcs800puri” tersebut di atas dengan tujuan untuk mendapatkan informasi tentang DNS Server dari domain presidensmy.info, yaitu

   1. Sahi78679.eart.orderboxdns.com;
   2. Sahi78679.mars.orderbox-dns.com;
   3. Sahi78679.venus.orderbox-dns; dan
   4. Sahi78679.mercury.orderbox-dns.com

f. Bahwa perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dengan mencari konfigurasi WHMCS (Web Host Manager Complete Solution) dengan mengakses URL www.techscape.co.id dan memilik menu login sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menemukan direktori my.technoscape.co.id (aplikasi membhosting management) dan mengubah tool WHMKiller guna mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape.co.id, menjalankan command Linux: cat/home/tech/www/myconfiguration.php melalui backdoor wso sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 berhasil mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape yaitu username: “techwhmsc” dan

password “y16=V=1J&mL(, menjalankan tool WHMKiller sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 mendapatkan database yang berisi sejumlah username dan password dari domain manager yang diserver www.techscape.co.id, melakukan akses ke server techscape.co.id sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 mendapatkan username dan password dari WHM control panel yaitu “root” dan “b4p4kg4nt3ngTIGA”, mengakses server techscape.co.id dengan ip address: 202.151.61.121 port 2086 melalui broser Mozilla Firefox, melakukan akses ke website www.enom.com selaku pihak domain register techscape.co.id dan selanjutnya melakukan login ke akun techscape dan password “tcs800puri” tanpa seijin pemiliknya yaitu CV Tecrhscape dengan tujuan untuk mendapatkan informasi tentang DSN Server dari domain presidenby.info dan mengakases website www.jatirejanetwork.com dengan tujuan mengganti DNS presidensby.info tanpa seijin pemilik dan pengelolanya yaitu saksi Eman Sulaiman Bin Enjen menjadi:

1. Id1.jatirejanetwork.com; dan
2. Id2jatirejanetwork.com.

Dan akibat perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada jam 22.45 WIB melakukan pembuatan (create) akun domain presidensby.info di server pihak perusahaan webhosting jatirejahost.com dan menempatkan sebuah file HTML “Jember Hacker Team” di server jatirejahost.com, sehingga ketika para user internet

tidak dapat mengakses konten website www.presidensby.info yang sebenarnya, akan tetapi konten yang terakses oleh para user adalah tampilan HTML “Jember Hacker Team.”

g. Bahwa selanjutnya saksi Grawas Sugiharto sebagai anggota Subdit I dan Cyber Crimer Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Mabes Polri melakukan penyelidikan atas illegal DNS rederection terhadap website www.presidenby.info dan hasil penyelidikan menemukan alamat tempat terdakwa Wildan Yani Ashari alias Yayan alias MJL007 terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan perbuatannya tersebut di atas yaitu Warnet CV Surya Infotama, Jalan Letjen Suprapto No. 169, Kebon Sari Jember, Jawa Timur. Kemudian saksi Grawas Sugiharto menyamar sebagai pengguna warnet dan melakukan wawancara dengan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada tanggal 25 Januari 2013 sekitar jam 18.00 WIB dan mengakui bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 memiliki akun nickname MJL007 di website forum hacker jember-hacker.org, selain itu saksi Grawas Sugiharto melihat langsung di komputer billing Warnet Surya Com tersimpan file database perusahaan hosting techscape.co.id dalam format file notepad (.txt). Sekitar jam 23.00 WIB saksi Grawas Sugiharto bersama Tim Penyidik Subdit IT dan Cyber Crime Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Mabes Polri

melakukan penangkapan terhadap Wildan Yani Ashari alias Yayan alias MJL007.

Perbuatan ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 sebagaimana diatur dan diancam pidana dalam Pasal 46 ayat (3) jo Pasal 30 ayat (3) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

ATAU

Kelima:

Bahwa ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada hari dan tanggal yang sudah tidak dapat diingat di pertengahan tahun 2012 sampai dengan tanggal 08 Januari 2013 sekira jam 22.45 WIB atau setidak-tidaknya pada waktu lain dalam tahun 2012 sampai dengan bulan Januari 2013 bertempat di CV Surya Infotama, Jalan Letjen Suprapto No. 169, Kebon Sari Kab. Jember, Jawa Timur atau setidak-tidaknya pada suatu tempat yang masih termasuk dalam daerah hukum Pengadilan Negeri Jember dengan sengaja dan atanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dan/atau dokumen elektronik. Perbuatan ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dilakukan dengan cara sebagai berikut:

a. Bahwa ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada waktu dan tempat sebagaimana tersebut di atas selaku operator *billing* Warnet Surya Com milik CV Surya Infotama, telah mengakses komputer dan/atau sistem elektronik www.jatirejanetwork.com dan

server my.techscape.co.id dengan menggunakan seperangkat komputer *billing* Warnet Surya Com milik CV Surya Infotama, sedangkan untuk software menggunakan tools berupa scrit khusus yang berbasiskan bahasa pemrograman PHP

b. Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dengan menggunakan nickname MJL007 terhadap website www.jatirejanetwork.com dengan *ip address* 210.247.249.58 bergerak dibidang pelayanan domain hosting milik dan dikelola saksi Eman Sulaiman bin Enjen yang dibeli dari saksi D.A. Giovanno Setyawardhana. Selanjutnya terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menemukan sebuah celah keamanan website www.jatirejanetwork.com, kemudian melakukan SQL Injection dan berhasil menanamkan sebuah backdoor berupa tools (software) yang berbasiskan bahsa pemrograman PHP yang bernama wso.php (web sell by orb) kemudian disimpan dalam harddisk komputer billing Warnet Surya Com terletak di drive D: Master pada folder: 001-MASTER SOFTWARE\009-TOOL\root.

c. Bahwa selanjutnya terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan keamanan server website yang sama ip addres-nya dengan techscape.co.id milik CV Techscape dengan *ip address* 210.247.249.58 dan menemukan celah keamanan, sehingga dapat disimpulkan bahwa server techscape.co.id memiliki celah keamanan yang sama. Kemudian terdakwa Wildan Yani Ashari alias

Yayan alias MJL007 melakukan reverse ip lookup terhadap website yang dimaksud dengan menggunakan tool on line (web based) www.yougetsignal.co, berhasil mendapatkan informasi bahwa website dimaksud memiliki *ip address* 210.247.249.58, lalu terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan pemeriksaan dan menemukan satu website yang merupakan webhosting yaitu www.techscape.co.id, selanjutnya melakukan pencarian terhadap direktori yang didalamnya terdapat konfigurasi WHMCS (WebHost Manager Complete Solution) yaitu aplikasi yang biasa digunakan untuk webhosting management, dan ditemukan direktori dimaksud adalah my.techscape.co.id.

d. Bahwa sekitar bulan November 2012 terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan akses terhadap website www.jatirejanetwork.com yang telah berhasil diterobos dengan teknik SQL Injection dan telah ditanamkan backdoor wso, selanjutnya menjalankan command linux: cat/home/tech/www/my/configuration.php melalui backdoor wso yang telah ditanam sebelumnya dan berhasil mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape yaitu username: “tech_whmcs dan password: “y16=V=1J&mL(“, kemudian terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menjalankan tool WHMKiller dari domain website www.jatirejanetwork.com untuk mendapatkan username dan password dari domain manager setiap

domain name yang ada di server webhosting dari WHM control panel antara lain username: “root” dan password: “b4p4kg4nt3ngTIGA” dengan port nomor: 2086, selanjutnya melakukan akses ke server techscape.co.id dengan ip address: 202.151.61.121 port: 2086 melalui browser Mozilla Firefox, setelah mendapatkan askes ke WHM control panel mengisi username: “root” dan password: “b4p4kg4nt3ngTIGA” kemudian menanamkan tool backdoor wso.php dengan cara melakukan uploading tool backdoor wso.php pada server techscape.co.id pada tanggal 16 November 2012 ja, 04.58:31 WIB. Agar backdoor tersebut tidak diketahui oleh admin techscape.co.id maka terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan perubahan nama (rename) terhadap tool dimaksud menjadi “domain.php” ditempatkan di sub direktori my.techscape.co.id/feeds/, sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dapat mengakses server techscape.co.id kapanpun melalui url: my.techscape.co.id/feeds/domaind.php dengan password: “yayan123”

e. Bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada tanggal 08 Januari 2008 sekitar jam 20.00 WIB melakukan akses ke website www.enom.com selaku domain registrar techscape.co.id dan selanjutnya melakukan login keakun techscape menggunakan username: techscape dan password: “tcs800puri” tersebut di atas dengan tujuan untuk mendapatkan informasi tentang DNS Server dari domain presidensmy.info, yaitu

1. Sahi78679.eart.orderboxdns.com;
2. Sahi78679.mars.orderbox-dns.com;
3. Sahi78679.venus.orderbox-dns; dan
4. Sahi78679.mercury.orderbox-dns.com

f. Bahwa perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dengan mencari konfigurasi WHMCS (Web Host Manager Complete Solution) dengan mengakses URL www.techscape.co.id dan memilik menu login sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 menemukan direktori my.technoscape.co.id (aplikasi membhosting management) dan mengubah tool WHMKiller guna mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape.co.id, menjalankan command Linux: cat/home/tech/www/myconfiguration.php melalui backdoor wso sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 berhasil mendapatkan username dan password dari database WHMCS yang dikelola pihak techscape yaitu username: "techwhmsc" dan password "y16=V=1J&mL(, menjalankan tool WHMKiller sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 mendapatkan database yang berisi sejumlah username dan password dari domain manager yang diserver www.techscape.co.id, melakukan akses ke server techscape.co.id sehingga terdakwa Wildan Yani Ashari alias Yayan alias MJL007 mendapatkan username dan password dari WHM control panel yaitu "root" dan "b4p4kg4nt3ngTIGA", mengakses

server techscape.co.id dengan ip address: 202.151.61.121 port 2086 melalui broser Mozilla Firefox, melakukan akses ke website www.enom.com selaku pihak domain register techscape.co.id dan selanjutnya melakukan login ke akun techscape dan password "tcs800puri" tanpa seijin pemiliknya yaitu CV Tecrhscape dengan tujuan untuk mendapatkan informasi tentang DSN Server dari domain presidenby.info dan mengakases website www.jatirejanetwork.com dengan tujuan mengganti DNS presidensby.info tanpa seijin pemilik dan pengelolanya yaitu saksi Eman Sulaiman Bin Enjen menjadi:

1. Id1.jatirejanetwork.com; dan
2. Id2jatirejanetwork.com.

Dan akibat perbuatan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada jam 22.45 WIB melakukan pembuatan (*create*) akun domain presidensby.info di server pihak perusahaan webhosting jatirejahost.com dan menempatkan sebuah file HTML "Jember Hacker Team" di server jatirejahost.com, sehingga ketika para user internet tidak dapat mengakses konten website www.presidensby.info yang sebenarnya, akan tetapi konten yang terakses oleh para user adalah tampilan HTML "Jember Hacker Team."

g. Bahwa selanjutnya saksi Grawas Sugiharto sebagai anggota Subdit I dan Cyber Crimer Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Mabes Polri melakukan penyelidikan atas illegal DNS rederection terhadap website www.presidenby.info dan hasil

penyelidikan menemukan alamat tempat terdakwa Wildan Yani Ashari alias Yayan alias MJL007 terdakwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan perbuatannya tersebut di atas yaitu Warnet CV Surya Infotama, Jalan Letjen Suprapto No. 169, Kebon Sari Jember, Jawa Timur. Kemudian saksi Grawas Sugiharto menyamar sebagai pengguna warnet dan melakukan wawancara dengan terdakwa Wildan Yani Ashari alias Yayan alias MJL007 pada tanggal 25 Januari 2013 sekitar jam 18.00 WIB dan mengakui bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 memiliki akun nickname MJL007 di website forum hacker jember-hacker.org, selain itu saksi Grawas Sugiharto melihat langsung di komputer billing Warnet Surya Com tersimpan file database perusahaan hosting techscape.co.id dalam format file notepad (.txt). Sekitar jam 23.00 WIB saksi Grawas Sugiharto bersama Tim Penyidik Subdit IT dan Cyber Crime Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Mabes Polri melakukan penangkapan terhadap Wildan Yani Ashari alias Yayan alias MJL007.

Perbuatan ia terdakwa Wildan Yani Ashari alias Yayan alias MJL007 sebagaimana diatur dan diancam pidana dalam Pasal 48 ayat (1) jo Pasal 32 ayat (1) Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

3. Tuntutan Penuntut Umum

a. Menyatakan terdakwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 bersalah melakukan tindak pidana dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun, sebagaimana diatur dalam Pasal 46 ayat (1) jo Pasal 30 ayat (1) Undang-undang Nomor 1 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam dakwaan alternatif kedua;

b. Menjatuhkan pidana terhadap terdakwa Wildan Yani Ashari alias Yayan alias MJL007 dengan pidana penjara selama 10 (sepuluh) bulan dikurangi selama terdakwa berada dalam tahanan dengan perintah terdakwa tetap ditahan dan denda sebesar Rp. 250.000,- (dua ratus lima puluh ribu rupiah) subsidair 1 (satu) bulan kurungan;

c. Menyatakan barang bukti berupa:
   1) 1 (satu) unit CPU merk Simbada warna abu-abu kapasitas 1 TB
   2) 1 (satu) unit CPU merk Powercase warna hitam kapasitas 80 GB, dikembalikan kepada yang berhak yaitu Warnet CV Surya Infotama Jl. Letjen Suprapto 169 Kebonsari Jember Jawa Timur
   3) 1 (satu) KTP atas nama Wildan Yani Ashari dikembalikan kepada terdakwa
   4) 1 (satu) keeping Compact Disk (CD) berisi file domain.php pada servertechscape

5) 1 (satu) keeping media cakram DVD berisi file akses IP Address 180.247.245.185 pada server alvindevelopment.com dirampas untuk dimusnahkan

d. Menetapkan agar terdakwa dibebani membayar biaya perkara sebesar Rp. 5.000,0 (lima ribu rupiah).

4. Amar Putusan

Menyatakan bahwa terdakwa Wildan Yani Ashari alias Yayan alias MJL007 telah terbukti secara sah meyakinkan bersalah melakukan tindak pidana dengan sengaja dan tanpa hak melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun;

a. Menjatuhkan pidana terhadap terdakwa oleh itu dengan pidana penjara selama 6 (enam) bulan dan denda Rp. 250.000,0 (dua ratus ribu rupiah) subsidair 15 hari kurungan;

b. Menetapkan bahwa masa penahanan yang telah dijalani oleh terdakwa dikurangi seluruhnya dari pidana yang dijatuhkan;

c. Memerintahkan agar terdakwa tetap berada dalam tahanan;

d. Menetapkan barang bukti berupa: 1 (satu) unit CPU merk Simbada warna abu-abu kapasitas 1 TB; 1 (satu) unit CPU merk Powercase warna hitam kapasitas 80 GB, dikembalikan kepada yang berhak yaitu Warnet CV Surya Infotama Jl. Letjen Suprapto 169 Kebonsari Jember Jawa; Timur1 (satu) KTP atas nama Wildan Yani Ashari dikembalikan kepada terdakwa; 1 (satu) keeping Compact Disk (CD) berisi file domain.php pada servertechscape; 1 (satu) keeping media cakram

DVD berisi file akses IP Address 180.247.245.185 pada server alvindevelopment.com dirampas untuk dimusnahkan;

e. Membebankan biaya perkara kepada terdakwa sebesr Rp. 5.000,- (lima ribu rupiah).

5. Analisis Kasus dan Pembahasan

Kasus pada putusan nomor 253/Pid/B/2013/PN JR merupakan kasus tindak pidana akses ilegal terhadap komputer, dimana terdakwa diancam pidana Pasal 50 jo Pasal 22 huruf b UU No. 36 Tahun 1999 tentang telekomunikasi; Pasal 46 ayat (1) jo Pasal 30 ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Pasal 46 ayat (2) jo Pasal 30 ayat (2) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Pasal 46 ayat (3) jo Pasal 30 ayat (3); dan Pasal 48 ayat (1) jo Pasal 32 ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Ancaman pidana tersebut didasarkan oleh hasil pembuktian tindakan pidana terdakwa, yaitu:

a. Penyidik

Penyidikan kasus pada putusan nomor 253/Pid/B/2013/PN JR dilakukan oleh tim penyidik Mabes Polri yang berkoordinasi dengan Polres Jember. Penyidikan dilakukan tim Mabes Polri karena objek dari kejahatan terdakwa adalah situs presiden SBY yang masuk dalam kategori keamanan nasional; sementara tim Mabes Polri berkoordinasi dengan Polres Jember karena tempat dilakukannya kejahatan berada di wilayah hukum Polres Jember. Penanganan *cyber crime* di Mabes Polri

berada di Direktorat Tindak Pidana Ekonomi Khusus (DITTIPPID EKSUS) di subdirektorat V.

Direktorat Tindak Pidana Ekonomi Khusus (DITTIPPID EKSUS) di subdirektorat V bertugas untuk melakukan penyelidikan dan penyidikan tindak pidana khusus, terutama kegiatan penyidikan yang berhubungan dengan teknologi informasi, telekomunikasi, serta transaksi elektronik. Berkaitan dengan tugas tersebut, fungsi dari satuan dari *Cyber Crime Direktorat Reserse Criminal* adalah:

1) Penyidikan kasus-kasus yang berhubungan dengan transaksi elektronik seperti *carding, money laundering*, pasar modal, pajak, perbankan, dll;
2) Penyidikan kasus-kasus yang berhubungan dengan teknologi komunikasi dan informasi meliputi penyandapan telepon, penggunaan VoIP, penipuan melalui telepon genggam;
3) Penyidikan kejahatan yang menggunakan fasilitas internet seperti *cyber gambling, cyber terrorism, cyber fraud, cyber sex, cyber narcotism, cyber smuggling, cyber attacks on critical infrastructure, cyber blackmail, cyber threatening*, pencurian dara, penghinaan dan/atau pencemaran nama baik, dll;
4) Penyidikan kejahatan komputer, seperti masuk ke sistem secara ilegal, *Ddos attack, hacking, tracking, phreaking*, membuat dan menyebarkan yang bersifat merusak, *malicous code all viruses, worm, rabbits, trojan*, dll;

5) Penyidikan kejahatan yang berhubungan dengan Hak Atas Kekayaan Intelektual (HAKI), *pirated software*, rekaman suara, merubah tampilan *website*, dll[41].

Penyidikan kasus pada putusan nomor 253/Pid/B/2013/PN JR diawali dari laporan saksi Eman Sulaeman sebagai pemilik *server* www.jatirejanetwork.com dan juga berdasarkan investigasi *online* yang diketahui telah terjadi tindak pidana *cyber* sekitar bulan Januari 2013 melalui interet dimana pelaku melakukan ilegal DNS *redirection* terhadap *website* www.presidensby.info sehingga *user* internet tidak dapat mengakses konten *website* tersebut yang sebenarnya, yang tampilan *homepage* gambar presiden SBY telah berubah tampilannya menjadi file HTML "Jember Hacker Team"[42].

Setelah mendapatkan laporan, maka dilakukan penyelidikan guna mengumpulkan informasi mengenai keberadaan/ tempat pelaku melakukan perbuatan tersebut dan akhirnya ditemukan alamat pelaku yaitu di Warnet CV Surya Infotama Jl. Letjen Suprapto 169 Kebonsari Jember Jawa Timur. Tim Mabes Polri selanjutnya berangkat ke Jember dan berkoordinasi dengan Polres Jember untuk mendapatkan bukti. Anggota tim melakukan penyamaran dan mendatangi Warnet CV Surya Infotama pada tanggal 25 Januari 2013 sekitar jam 18.00 WIB. Anggota tim yang menyamar kemudian melakukan wawancara langsung dengan pelaku Wildan Yani Ashari dan dari pelaku diperoleh

41 *https://www.polri.go.id/* download 12 April 2017
42 Hasil wawancara dengan Grawas Sugiharto, selaku penyidik Mabes Polri

pernyataan langsung bahwa pelaku adalah *hacker* dengan *nickname* MJL007 dan aktif di forum *hacker Jember-hacker.org*. Dalam penyamaran tersebut, anggota tim juga melihat langsung di komputer billing Warnet CV Surya Com tersimpan file database perusahaan hosting techscape.co.id dalam format file notepad (.txt). Adanya fakta-fakta tentang tindak kejahatan ilegal akses terhadap komputer, maka tim Mabes Polri yang sudah dilengkapi surat perintah tugas, surat perintah penyidikan, surat perintah penggeledahan, dan surat perintah penyitaan, dengan didampingi oleh satu orang anggota Polres Jember melakukan penangkapan, penggeledahan dan penyataan barang bukti. Selain itu, saat ditangkap pelaku mengakui bahwa dirinya pemilik nickname MJL007 dan yang melakukan tindak kejahatan tersebut[43].

Pembuktian kasus pada putusan nomor 253/Pid/B/2013/PN JR dari perspektif penyidik yang telah dijabarkan di atas, diperkuat oleh ungkapan dari para penyidik yang terlibat dalam kasus tersebut, yaitu:

> "*Jadi setelah kami mengetahui posisi pelaku, kami segera meluncur ke TKP dan saya bertugas melakukan penyamaran. Dalam penyamaran, pelaku mengaku kalau dirinya hacker dan membuktikan dengan "prestasinya" telah hack situsnya SBY…bukti sudah ada ya tim langsung turun melakukan penggeledahan, penangkapan, dan penyitaan barang bukti*."[44]

> "*Begitu kami dapat kode dari rekan Grawas, kami langsung ke TKP dan menunjukkan surat-surat terkait. Dari penggeledahan kami menyita barang bukti CPU dan KTP. Kami menerima pengakuan pelaku atas tindak pidana yang diperbuat*."[45]

---

43 Hasil wawancara dengan Bp. Grawas Sugiharto, selaku penyidik Mabes Polri

44 *Ibid*

45 Hasil wawancara dengan Bp. Immanuel P. Lumban Tobong, selaku penyidik Mabes Polri

"*Pemeriksaan barang bukti memang ditemukan data-data log yang dilalui pelaku dan membuktikan adanya ilegal DNS redirection pada situs presiden SBY.*"[46]

Dari penjabaran di atas dapat disimpulkan bahwa pembuktian kasus pada putusan nomor 253/Pid/B/2013/PN JR (kasus tindak pidana akses ilegal terhadap komputer) dari perspektif penyidik sebagai berikut:

1) Keterangan saksi, yaitu saksi dari penyidik mengenai adanya tindak pidana akses ilegal terhadap komputer yang dilakukan oleh Wildan Yani Ashari alias MJL007;
2) Barang bukti berupa:
   a) 1 (satu) unit CPU warna merah merek Power Up dengan 1 (satu) buah internal harddisk merek Maxtor s/n: 9QZB887G kapasitas 80 GB;
   b) 1 (satu) unit CPU warna hitam merah merek Simbadda dengan 1 (satu) buah internal harddisk merek Seagater s/n: 5VP6GX7R kapasitas 1 TB;
   c) 1 (satu) keeping CD merek IZUMI Kapasitas 700 MB s/n: CD-R IZ-1; dan
   d) 1 (satu) keeping DVD Primary Image warna putih kapasitas 4,76 GB s/n: 2117E22230913821.
3) Dokumen elektronik berupa file database perusahaan hosting techscape.co.id dalam format file notepad (.txt);

[46] Hasil wawancara dengan Bp. Aditya Cahya, selaku penyidik Mabes Polri

4) Pemeriksaan digital forensik pada barang bukti menunjukkan adanya data-data l*og* yang dilalui pelaku dan membuktikan adanya ilegal DNS *redirection* pada situs presiden SBY; dan
5) Pada saat penangkapan pelaku mengakui bahwa MJL007 adalah dirinya dan juga yang melakukan ilegal DNS *redirection* pada situs presiden SBY.

Pembuktian kasus pada putusan nomor 253/Pid/B/2013/PN JR (kasus tindak pidana akses ilegal terhadap komputer) oleh penyidik jika diklasifikasikan ke dalam bukti elektronik mencakup:

1) *Real evidence,* yaitu hasil rekamanan langsung dari suatu aktifitas elektronik, hasil penghitungan atau analisa oleh suatu sistem komputer yang telah bekerja sesuai dengan prosedur perangkat lunak yang digunakan untuk pemrosesan data atau informasi, rekaman data log dari sebuah server dalam internet, atau juga dapat berbentuk salinan (*receipt*) dari suatu peralatan seperti hasil rekaman kamera yang menggunakan sensor. *Real evidence* ini meliputi file database perusahaan hosting techscape.co.id dalam format file notepad (.txt) dan pemeriksaan digital forensik pada barang bukti menunjukkan adanya data-data l*og* yang dilalui pelaku dan membuktikan adanya ilegal DNS *redirection* pada situs presiden SBY.
2) *Hearsay evidence*, yaitu dokumen atau rekaman yang merupakan hasil dari pemrosesan dengan menggunakan komputer yang

kesemuanya adalah salinan atas sebuah informasi di atas kertas. *Hearsay evidence* meliputi BAP sanksi, BAP saksi ahli, BAP terdakwa, dan BAP barang bukti, serta barang bukti CD yang berisi file domain.php pada servertechscape dan DVD yang berisi file akses IP Address 180.247.245.185 pada server alvindevelopment.com

3) *Derived evidence*, yaitu kombinasi antara *real evidence* dan *hearsay evidence*. Penggunaan data atau pesan elektronik sebagai barang bukti di pengadilan dicari ada tidaknya suatu hubungan antara keduanya. *Derive evidence* meliputi komputer yang digunakan untuk melakukan tindak pidana dan ahli TI.

b. Jaksa Penuntut Umum

Pasal 1 ayat (1) UU No. 16 Tahun 2004 tentang Kejaksaan Republik Indonesia, yang dimaksud dengan jaksa adalah

> "Jaksa adalah pejabat fungsional yang diberi wewenang oleh undang-undang untuk bertindak sebagai penuntut umum dan pelaksana putusan pengadilan yang telah memperoleh kekuatan hukum tetap serta wewenang lain berdasarkan undang-undang."

Selanjutnya Pasal 1 ayat (2) menjelaskan bahwa Jaksa Penuntut Umum (JPU) adalah "Penuntut Umum adalah jaksa yang diberi wewenang oleh Undang-Undang ini untuk melakukan penuntutan dan melaksanakan penetapan hakim." Tugas dan wewenang jaksa di bidang pidana menurut Pasal 30 ayat (1) adalah:

1) Melakukan penuntutan;

2) Melaksanakan penetapan hakim dan putusan pengadilan yang telah memperoleh kekuatan hukum tetap;
3) Melakukan pengawasan terhadap pelaksanaan putusan pidana bersyarat, putusan pidana pengawasan, dan keputusan lepas bersyarat;
4) Melakukan penyidikan terhadap tindak pidana tertentu berdasarkan undang-undang;
5) Melengkapai berkas perkara tertentu dan untuk itu dapat melakukan pemeriksaan tambahan sebelum dilimpahkan ke pengadilan yang dalam pelaksanaannya dikoordinasikan dengan penyidik.

Berkaitan dengan kasus pada putusan nomor 253/Pid/B/2013/PN JR, penyidikan yang dilakukan oleh aparat polisi (tim *cyber crime* dari Mabel Polri) diperoleh bukti-bukti yang memadai bahwa telah terjadi tindak pidana akses ilegal terhadap komputer yang dilakukan oleh Wildan Yani Ashari alias Yayan alias MJL007. Selanjutnya penyidik melanjutkan proses penyidikan dengan membuat berita acara (pemberkasan perkara) untuk diserahkan kepada penuntut umum.

Selanjutnya jaksa selaku penuntut umum akan membuat surat dakwaan, dimana dalam surat dakwan tersebut didasari atas alat-alat bukti yang telah diteliti, diperiksa dan disimpan oleh jaksa. Selain itu, sistem pembuktian didasarkan pada KUHP dan Pasal 183 KUHAP

yakni minimal ada dua alat bukti yang sah menurut UU, yang apabila telah memenuhi syarat-syarat perkara tersebut maka akan diteruskan pada proses pemeriksaan di sidang pengadilan[47].

Kasus pada putusan nomor 253/Pid/B/2013/PN JR, JPU Pengadilan Negeri Jember mengajukan tuntutan yang didasari oleh keyakinan telah terjadi tindak pidana akses ilegal terhadap komputer, berupa fakta-fakta yang didapat dari bukti, barang bukti dan alat bukti[48].

1) Bukti adalah suatu hal atau peristiwa yang cukup untuk memperlihatkan kebenaran suatu hal atau peristiwa[49]. Dengan demikian, BAP saksi, BAP tersangka, BAP ahli atau laporan ahli, surat dan barang bukti yang disita, kesemuanya mempunyai nilai sebagai bukti.
2) Barang bukti adalah benda baik yang bergerak atau tidak bergerak, yang berwujud maupun yang tidak berwujud yang mempunyai hubungan dengan tidak pidana yang terjadi. Dalam kasus ini, diperoleh 5 (lima) barang bukti yaitu CPU, KTP atas nama Wildan Yani Ashari, CD berisi file domain.php pada servertechscape, dan media cakram DVD berisi file akses IP Address 180.247.245.185 pada server alvindevelopment.com.

---

47 M.Yustin A., *op cit*

48 Hasil wawancara dengan Ibu Asih, selaku JPU di Kejaksaan Negeri Jember Tindak Pidana Khusus

49 *https://www.kbbi.web.id/bukti* download 12 April 2017

3) Alat bukti sesuai Pasal 183-184 KUHAP dan Pasal 5 UU ITE, yang menjelaskan bahwa:

Pasal 183 KUHAP

"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 terdakwalah yang bersalah melakukannya."

Pasal 184 ayat (1) KUHAP

"alat bukti yang sah adalah keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa".

Pasal 5 UU ITE

Ayat (1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

Ayat (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.

Ayat (3) Informasi Elektronik dan/atau Dokumen Eletronik dinyatakan sah apabila menggunakan Sistem, Elektronik sesuai dengan ketentuan yang diatur dalam Undang-undang ini.

Ayat (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 notaril atau akta yang dibuat oleh pejabat pembuat akta.

Dari uraian di atas, tuntutan JPU terhadap kasus tindak pidana akses ilegal terhadap komputer pada putusan nomor 253/Pid B/2013/PN JR adalah pembuktian tindak pidana tersebut sudah sesuai

dengan ketentuan hukum pembuktian pada KUHAP dan UU ITE. Hal tersebut seperti kutipan pernyataan dari JPU di bawah ini:

> "*Pada dasarnya, tuntutan yang kami acukan sudah sesuai dengan peraturan yang berlaku, baik untuk sistem pembuktiannya, alat bukti, cara menggunakan alat bukti dan nilai, dan kekuatan pembuktian dari masing-masing alat bukti yang ditemukan. Sudah sesuai aturan*."[50]

Pembuktian tindak pidana akses ilegal terhadap komputer pada putusan nomor 253/Pid B/2013/PN JR sudah sesuai dengan ketentuan hukum pembuktian pada KUHAP dan UU ITE, yaitu:

1) Pasal 183 dan 184 ayat (1) KUHAP: ditemukan lebih dari dua alat bukti yang sah dan menyakinkan bahwa tindak pidana akses ilegal terhadap komputer benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya. Dua alat bukti tersebut adalah keterangan saksi, keterangan saksi ahli, dokumen elektronik, barang bukti, dan pengakuan terdakwa.
2) Pasal 5 UU ITE: ditemukannya bukti dokumen elektronik baik *real evidence*, *hearsay evidence*, dan *derived evidence*.
3) Pasal 50 *jo* Pasal 22 huruf b UU No. 36/1999 tentang Komunikasi

> Pasal 50:
> Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dana tau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).
> Pasal 22 huruf b:
> Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi: … huruf b. akses ke jasa telekomunikasi; dan atau

[50] Hasil wawancara dengan Ibu Asih, selaku JPU di Kejaksaan Negeri Jember Tindak Pidana Khusus

4) Pasal 46 ayat (1) *jo* Pasal 30 ayat (1) UU ITE

Pasal 46 ayat (1):
Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).

Pasal 30 Ayat (1):
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

5) Pasal 46 ayat (2) *jo* Pasal 30 ayat (2) UU ITE

Pasal 46 ayat (2):
Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp. 700.000.000,00 (tujuh ratus juta rupiah).

Pasal 30 Ayat (2):
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

6) Pasal 46 ayat (3) *jo* Pasal 30 ayat (3) UU ITE

Pasal 46 ayat (3):
Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 800.000.000,00 (delapan ratus juta rupiah).

Pasal 30 Ayat (3):
Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

7) Pasal 48 ayat (1) *jo* Pasal 32 ayat (1) UU ITE

Pasal 48 ayat (1):

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).

Pasal 32 ayat (1):
Setiap Orang dengan sengaja dan tanpa haka tau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

Dengan kata lain pembuktian tindak pidana akses ilegal terhadap komputer pada putusan nomor 253/Pid B/2013/PN JR sudah sesuai dengan ketentuan hukum pembuktian pada KUHAP dan UU ITE, karena memenuhi unsur objektif dan unsur subjektif dari tindak pidana akses ilegal terhadap komputer.

c. Ahli IT

Keterangan ahli IT dalam proses pemeriksaan perkara *cyber crime* baik pada tahap pemeriksaan penyidikan maupun pada pemeriksaan di sidang pengadilan sangat penting dan dibutuhkan, terutama untuk membantu penyidik, penuntut umum ataupun hakin dalam mengungkapkan suatu kasus *cyber crime*. Pentingnya keterangan ahli IT diperkuat dalam Pasal 184 KUHAP yang menjelaskan bahwa keterangan ahli merupakan salah satu dari alat bukti yang sah.

Untuk kasus pada putusan nomor 253/Pid B/2013/PN JR, saksi ahli berasal kalangan akademisi. Saksi adalah bekerja di Fakultas

Teknik Informatika Universitas Bina Nusantara, serta menjabat sebagai *Concentration Content Coordinator Software Engenering* (jabatan struktural) dan Asisten Ahli (jabatan fungsional). Saksi ahli ini memiliki keahlian di bidang *Advanced Topid Software Enginering Current Popular IT*, Algoritma Pemprograman dan *Object Oriented Software Engenering*.

Saksi ahli IT ini menjelaskan bahwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan akses ilegal terhadap komputer dengan cara menggunakan tools WSO WHMKiller, memang dapat dilakukan oleh terdakwa untuk memasuki, menerobos sistem server Techscape.co.id dan sistem server jatirejahost.com serta illegal DNS redirection terhadap domain presidensby.info. Dengan tools WSO, maka seluruh manajemen file, manajemen database sebuah web hosting yang resmi dari pemilik web hosting dan dengan tools WHM Killer, maka bisa didapatkan username dan password seluruh alamat domain pada suatu web hosting server tanpa melalui sistem resmi pemilik web hosting.[51] Secara singkat, ahli TI ini menjelaskan bahwa "*pemeriksaan barang bukti memang terdapat data-data log yang dilalui pelaku dan membuktikan adanya ilegal DNS redirection pada situs presiden SBY*"[52].

Berdasarkan penjabaran di atas, maka pembuktian pada tindak pidana akses ilegal terhadap komputer pada putusan nomor 253/Pid B/2013/PN JR

[51] Hasil wawancara dengan Aditya Kurniawan, selaku Ahli TI
[52] Aditya Kurniawan, *op cit*

menurut penyidik, JPU dan ahli TI memadai untuk menuntut Wildan Yani Ashari alias Yayan alias MJL007 sebagai terdakwa dalam melakukan tindak pidana akses ilegal terhadap komputer, berupa ilegal DNS *redirection* pada situs presiden SBY. Pembuktian yang dilakukan sudah mengacu peraturan yang berlaku, yaitu Pasal 183-184 KUHAP dan Pasal 5 UU ITE.

Berdasarkan analisis pembuktian tindak pidana akses ilegal terhadap komputer oleh penyidik dalam Putusan Hakim No. 253/Pid B/2013/PN JR diketahui telah ditemukan alat-alat bukti yang sah dan menyakinkan sesuai Pasal 184 KUHAP sehingga menjadi dasar bagi majelis hakim dalam mencari dan meletakkan kebenaran yang akan dijatuhkan dalam putusannya terhadap tindak pidana tersebut. Adapun alat-alat bukti tersebut meliputi:

1. Keterangan saksi, yaitu saksi korban (pemilik sekaligus pengelola Warnet CV Surya Com) dan saksi penyidik. Keterangan saksi ini menjelaskan adanya tindak pidana akses ilegal terhadap komputer yang dilakukan oleh Wildan Yani Ashari alias MJL007.
2. Keterangan ahli, yaitu keterangan ahli TI yang berasal kalangan akademisi dan bekerja di Fakultas Teknik Informatika Universitas Bina Nusantara, serta menjabat sebagai *Concentration Content Coordinator Software Engenering* (jabatan struktural) dan Asisten Ahli (jabatan fungsional), dengan keahlian di bidang *Advanced Topid Software Enginering Current Popular IT*, Algoritma Pemprograman dan *Object Oriented Software Engenering*. Keterangan ahli TI ini menjelaskan bahwa Wildan Yani Ashari alias Yayan alias MJL007 melakukan akses ilegal terhadap

komputer dengan cara menggunakan tools WSO WHMKiller, memang dapat dilakukan oleh terdakwa untuk memasuki, menerobos sistem server Techscape.co.id dan sistem server jatirejahost.com serta illegal DNS redirection terhadap domain presidensby.info. Dengan tools WSO, maka seluruh manajemen file, manajemen database sebuah web hosting yang resmi dari pemilik web hosting dan dengan tools WHM Killer, maka bisa didapatkan username dan password seluruh alamat domain pada suatu web hosting server tanpa melalui sistem resmi pemilik web hosting.

3. Surat, yaitu BAP saksi, BAP ahli, BAP terdakwa, dan BAP barang bukti.
4. Petunjuk, yaitu ditemukannya barang bukti dan alat bukti. Barang bukti berupa dokumen elektronik (file database perusahaan hosting techscape.co.id dalam format file notepad (.txt)); sementara alat bukti berupa komputer (satu unit CPU warna merah merek Power Up dengan satu buah internal harddisk merek Maxtor s/n: 9QZB887G kapasitas 80 GB; satu unit CPU warna hitam merah merek Simbadda dengan satu buah internal harddisk merek Seagater s/n: 5VP6GX7R kapasitas 1 TB; satu keeping CD merek IZUMI Kapasitas 700 MB s/n: CD-R IZ-1; dan satu keeping DVD Primary Image warna putih kapasitas 4,76 GB s/n: 2117E22230913821)
5. Keterangan terdakwa, yaitu pada saat penangkapan pelaku mengakui bahwa MJL007 adalah dirinya dan juga yang melakukan ilegal DNS *redirection* pada situs presiden SBY.

B. Faktor yang Menghambat Pembuktian Tindak Pidana Akses Ilegal terhadap Komputer

Terdapat beberapa faktor yang menghambat pembuktian tindak pidana akses ilegal terhadap komputer. Beberapa faktor tersebut adalah:

1. Kelemahan infrastruktur

   Untuk mengungkap kejahatan *cyber* membutuhan teknologi yang canggih, dan hingga hari teknologi ini masih terbatas dimana hanya dimiliki oleh mabes Polri serta teknologi baru terintegrasi ke 15 Polda yang di Indonesia. Oleh karena itu, proses penyidikan dan penyelidikan dalam rangka pembuktian kurang efisien.

2. Keterbatasan personel penegak hukum

   Terbatasnya personel penegak hukum (penyidik maupun jaksa penuntut umum) yang memiliki keahlian dan ketrampilan di bidang kejahatan *cyber*, sehingga dapat menghambat proses pembuktian. Selain itu, pemahaman dan keahlian para penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan kejahatan cyber masih terbatas[53].

[53] Evi Lestari Situmorang, 2014, Kajian Yuridis Pembuktian Kejahatan Mayatara (Cybercrime) dalam Lingkup Transnasional (Studi Putusan), Jurnal, Sumatera: FH Universitas Sumatera Utara. https://jurnal.usu.ac.id/index.php/jmpk/article/viewFile/8413/3651 download 12 Desember 2017