Keamanan Data User Pada Jaringan Wirelles Menggunakan Two Factor, Password Dan Mac Address Filtering Di Jurusan Teknik Komputer

Slamet Widodo [1)], Adi Sutrisman [2)], M.Miftakhul Amin[3)], Muhammad fernaldo harefa[4)] , Muhammad Aulia Farhan[5], Muhammad Reinaldo[6)]
[1,2,3,4,5,6*)] Jurusan Teknik Komputer, Politeknik Negeri Sriwijaya

email: slametwidodo@polsri.ac.id,adistra@polsri.ac.id,m.amin@polsri.ac.id, harefa@gmail.com ,m.farhan@gmail.com,m.reinaldo@gmail.com

Abstract

Wireless network in the form of hotspot technology. Hotspot networks are an important requirement in activities implemented in universities. Frequent attacks that disrupt the internet network such as Wireless Hacking. This study discusses user data security applications and wireless security systems using two factors, passwords and MAC address filters in the computer engineering department. Therefore, to overcome this problem, network security was built with firewall settings, namely filter rules and NAT. Based on these problems, the discussion that will be reviewed is about making user data security applications that are useful for accommodating the user's MAC address and making hotspots on Mikrotik, and testing the designed hotspot network. Based on the test results, it can be concluded that the firewall can overcome illegal hotspot users in the MikroTik hotspot. With the development of user data security applications and internet security using a firewall, setting the filter rules and NAT helps users to minimize the occurrence of illegal users. Firewalls are able to filter access to a computer using a list of permissions (permissions list) that is made based on the MAC address. By registering the MAC-Address, illegal users who are not registered in the network cannot easily access wireless networks in the Computer Engineering department.
Keywords: Firewall, Hotspot, Mac-Address-Filter, Mikrotik.

Abstrak

Wireless berupa teknologi hotspot. Jaringan hotspot menjadi kebutuhan penting dalam aktivitas yang diterapkan di Perguruan Tinggi. Sering terjadi serangan yang mengganggu jaringan internet seperti Wireless Hacking. Penelitian ini membahas tentang aplikasi keamanan data user dan sistem keamanan wireless menggunakan two factor, password dan MAC address filter di jurusan teknik komputer. Oleh karena itu, untuk mengatasi masalah tersebut dibangun keamanan jaringan dengan pengaturan firewall yaitu filter rule dan NAT. Berdasarkan masalah tersebut, pembahasan yang akan diulas yaitu mengenai pembuatan aplikasi keamanan data user yang berguna untuk menampung MAC address pengguna dan pembuatan hotspot pada mikrotik, dan melakukan pengujian terhadap jaringan hotspot yang dirancang. Berdasarkan hasil pengujian dapat disimpulkan bahwa pada firewall, dapat mengatasi user hotspot illegal yang ada pada hotspot mikrotik. Dengan terbangunnya aplikasi keamanan data user dan keamanan internet menggunakan firewall yaitu melakukan setting pada filter rules dan NAT membantu pengguna untuk meminimalisir terjadinya user illegal. Firewall mampu melakukan penyaringan akses ke dalam sebuah komputer menggunakan daftar perijinan (permissions list) yang dibuatkan berdasarkan MAC address. Dengan dilakukannya pendaftaran pada MAC-Address, user illegal yang tidak terdaftar di dalam jaringan tidak dapat dengan mudah untuk mengakses jaringan wireless di jurusan Teknik Komputer..
Kata Kunci : Firewall, Hotspot, Mac-Address-Filter, Mikrotik.

1. PENDAHULUAN

Keamanan jaringan adalah masalah utama komputasi karena banyak jenis serangan meningkat dari hari ke hari. Dalam jaringan ad-hoc seluler, node bersifat independen. Melindungi keamanan komputer dan jaringan adalah masalah penting. [1]

Karena peningkatan layanan berbasis internet, ukuran lalu lintas data jaringan menjadi sangat besar dan kompleks sehingga sangat sulit untuk diproses dengan alat pemrosesan data tradisional.[2] Jaringan wireless merupakan teknologi terbaru yang digunakan sebagai pengganti apabila kondisi lingkungan tidak memungkinkan menggunakan teknologi kabel, dengan kata lain dapat menjadi alternatif. [3] Jaringan Wifi memiliki lebih banyak kelemahan dibanding dengan jaringan kabel. Saat ini perkembangan teknologi wifi sangat signifikan sejalan dengan kebutuhan sistem informasi yang mobile. Banyak penyedia jasa wireless seperti hotspot komersil, ISP, Warnet, kampus?kampus maupun perkantoran sudah mulai memanfaatkan wifi pada jaringan masing masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan wireless tersebut.[4]

Keamanan jaringan menjadi lebih penting bagi pengguna komputer pribadi, organisasi, dan militer. Dengan munculnya internet, keamanan menjadi perhatian utama dan sejarah keamanan memungkinkan pemahaman yang lebih baik tentang munculnya teknologi keamanan.[5] Kinerja suatu jaringan Wi-Fi, misalnya pada suatu gedung, dapat diketahui dari penerimaan sinyal yang diterima oleh pengguna dari access point (AP) Wi-Fi. Tentunya penerimaan sinyal yang naik turun atau yang lemah tidak dikehendaki pada koneksi Internet. Apabila penempatan AP di dalam suatu gedung Terdapat dilakukan secara tepat maka kinerja jaringan Wi-Fi akan lebih optimal. [6]

Masalah utama di Jaringan Wireless adalah keamanan, metode yang sering digunakan adalah dengan otentikasi. Dalam penelitian ini dilakukan percobaan penetrasi protocol enkripsi WEP, WPA dan RADIUS. [7]. Jaringan wireless merupakan jaringan yang banyak digunakan pada institusi maupun tempat umum. Jaringan wireless memiliki sistem keamanan seperti WEP, WPAPSK/WPA2PSK, dan MAC Address filtering.Walaupun memiliki sitem keamanan jaringan wireless masih dapat di diserang oleh para attacker dengan menggunakan jenis serangan Cracking the Encryption dan bypassing WLAN Authentication.[8]

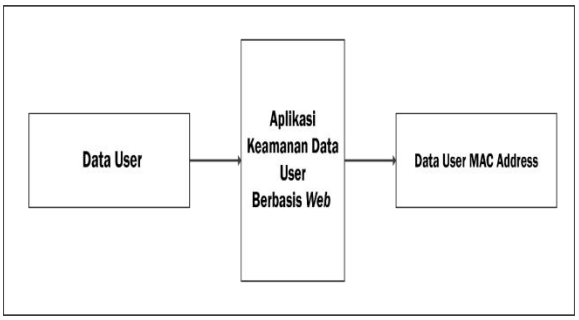
Karena WEP adalah keamanan WLAN awal dan yang disebut mekanisme dari semua protokol tersebut di atas, ditujukan untuk mencakup dalam perspektif yang lebih luas dari WPA/WPA2 dan RSN. Beberapa kelemahan serius diidentifikasi oleh cryptanalysts di WEP, dan WEP digantikan oleh Wi-Fi Protected Access (WPA) pada tahun 2003, dan kemudian dengan standar penuh IEEE 802.11i RSN (juga dikenal sebagai WPA2) pada tahun 2004 diratifikasi.[9]. Pada jaringan nirkabel, masalah keamanan memerlukan perhatian yang lebih serius, mengingat media transmisi datanya adalah gelombang radio yang bersifat *broadcast*.

Permasalahan penelitian ini berlatar belakang di jurusan Teknik Komputer keamanan jaringan *wireless* masih menggunakan WEP, WPA, WPA2, dan *Hotspot login*, yang dimana untuk mengaksess jaringan *wireless* tersebut hanya dengan memasukkan *password* yang di tentukan oleh administrator jaringan sehingga siapa saja yang mengetahuinya bisa mengakses jaringan *wireless* tersebut dengan tanpa hambatanminat belajar peserta didik.

2. METODELOGI PENELITIAN

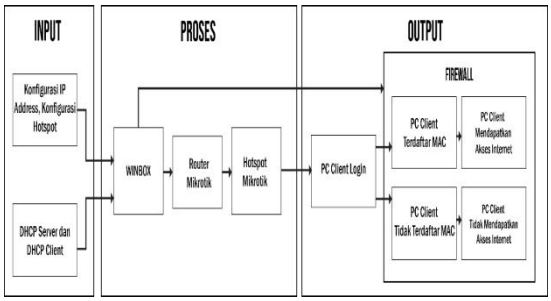
Dalam perancangan keamanan jaringan komputer tujuan untuk membuat suatu aplikasi keamanan data *user* berbasis web untuk membatasi pengguna jaringan *wireless* dengan menggunakan keamanan pada WPA-PSK dan MAC *Address filtering*.

Perancangan sistem yang akan di bahas adalah mengenai bagaimana proses penggunaan aplikasi keamanan data *user* dan juga proses pembuatan keamanan jaringan komputer untuk membuat MAC *Address Filter* menggunakan *Firewall*. Berikut adalah diagram blok perancangan sistem dapat dilihat pada Gambar 3.1 dan Gambar 3.2.



Gambar 3.2 Diagram Blok Aplikasi Keamanan Data User

Dari Gambar 3.2 diatas terdapat sistem kerja yang berupa *Input, Process* dan *Output.* Untuk *input-nya* berupa Data User yang di kumpulkan. Untuk *Proses-nya* yaitu menggunakan aplikasi keamanan data user berbasis *web* yang kemudian menghasilkan data keluaran (*output*) berupa data *user* MAC *Address*

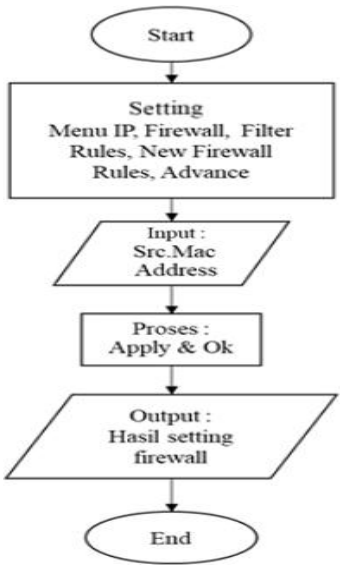


Gambar 3.3 Diagram Blok Sistem Keamanan

Dari Gambar 3.3 diatas terdapat sistem kerja yang berupa *Input, Process* dan *Output.* Untuk *input*-nya berupa alamat IP ke *router*, setelah itu mengatur DHCP *Server* pada *router*, dan *setting* DHCP *Client* pada perangkat yang terhubung untuk mendapatkan alamat IP secara otomatis. Untuk *proses-nya* berupa winbox yang digunakan untuk melakukan konfigurasi pada *router* mikrotik dan pembangunan *hotspot* mikrotik. *Output* nya berupa PC *Client* login menggunakan username dan password. PC *Client* dengan kondisi memiliki MAC *Address* yang terdaftar di dalam MAC Address Filter dan PC Client dengan kondisi memiliki MAC Address yang tidak terdaftar di dalam MAC Address Filter. Lalu dengan ditambahkannya *setting*-an *firewall* MAC *Address Filter*, PC *Client* berhasil *login* dan mendapatkan hak akses Internet dan PC *Client* yang tidak terdaftar MAC Address-nya berhasil login tetapi tidak bisa mendapatkan hak akses Internet.

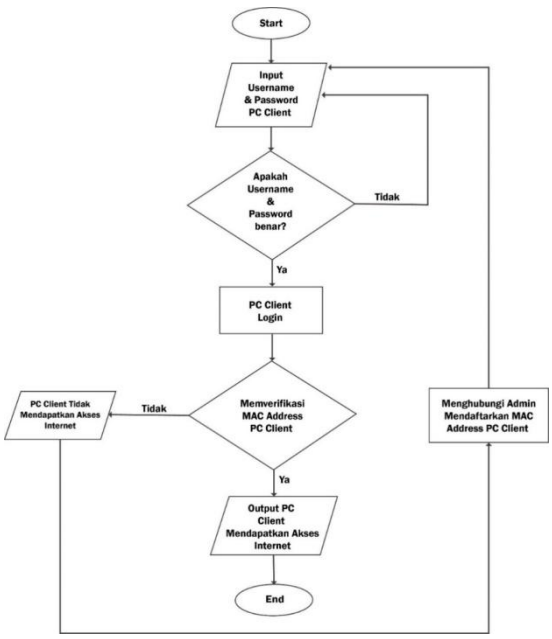
Perancangan Sistem Keamanan Menggunakan *Firewall*

Metode proteksi *firewall* ini adalah sebuah cara untuk mengamankan keamanan *internet*. Pengguna bisa langsung menggunakan *internet*, dengan metode proteksi yang diterapkan ini pengguna harus terlebih dahulu meminta dibuatkan *username* dan *password* kepada admin untuk mengakses *internet* yang ada di Jurusan Teknik Komputer. Berikut adalah proses keamanan *internet* menggunakan proteksi *firewall* :



Gambar 3.4 MAC *Address Filter*

Berikut adalah hasil dari dilakukannya penambahan proteksi pada *firewall* pada gambar 3.5 :

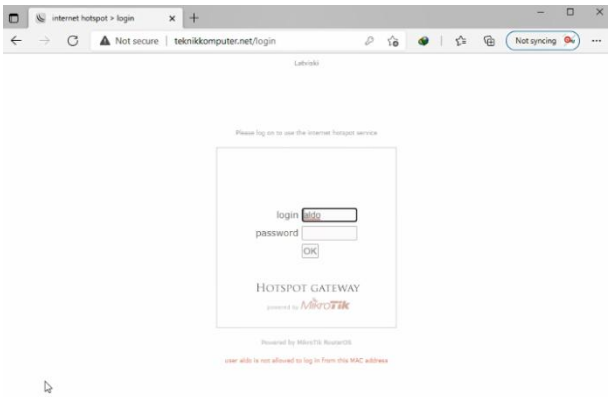


Gambar 3.5 Hasil *Login* Setelah dilakukan *setting* pada *firewall*

Pada awalnya sebelum ada setting pada *firewall* ketika ada *user* pada *client* yang secara *illegal* dapat dengan mudah mengambil alih hak autoritas *user* yang sudah memiliki *user* secara *legal*. Sehingga pemilik *user* yang asli akan kehilangan otoritasnya dalam bebas mengakses internet dikarenakan autoritas user telah diambil secara *illegal*. Namun ketika sudah dibangun sistem keamanan dengan memanfaatkan *firewall* ini berjalan, sehingga ketika dilakukan *login* dengan MAC *address filter* secara otomatis tidak akan bisa dengan mudah *login* ke jaringan dan hak autoritas pemilik *user* asli dapat dikembalikan. Oleh karena itu, agar dapat *login* MAC *address* harus berbeda dan otomatis *username* dan *password* juga harus berbeda dan harus mendaftar dahulu kepada *administrator* jaringan.

3. HASIL DAN PEMBAHASAN

Setelah semua *setting*-an *firewall* selesai selanjutnya dilakukan tes jaringan *hotspot*. Pertama login PC *Client1* terlebih dahulu menggunakan *hotspot ether2*. Untuk hasilnya bisa dilihat pada gambar 4.1 dan 4.2 berikut ini

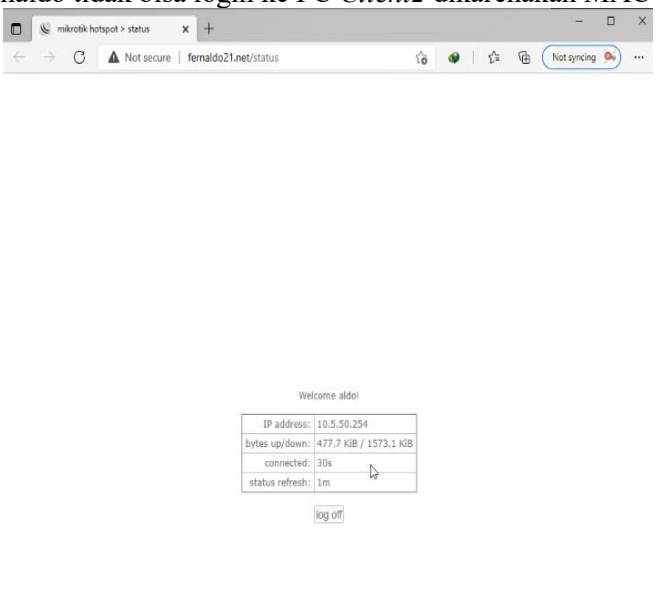


Gambar 4.1 *Login* PC *Client1 user*

Disini *user* tidak bisa login ke PC *Client 1* dikarenakan MAC *Address*-nya berbeda.

Pengujian User Login

Disini *user* fernaldo tidak bisa login ke PC *Client2* dikarenakan MAC *Address*-nya berbeda.



Gambar 4.2 *Login* PC *Client2 user*

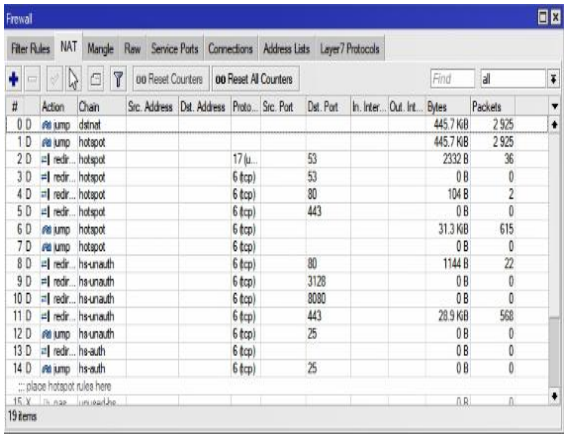
Disini *user* aldo bisa *login* ke PC *Client 2* dikarenakan MAC *Address*-nya sama dengan MAC *Address* PC *Client2*. Jika *hotspot* telah di konfigurasi pada mikrotik, untuk dapat masuk ke jaringan dan *login* pada domain *hotspot* menggunakan *user profile* yang telah dibuat yang MAC *Address-nya* sudah terdaftar dan diakses menggunakan PC yang MAC *Address-nya* sama. Untuk hasil pengujian tes jaringan *hotspot* bisa dilihat pada tabel 4.2. Hasil Pengujian :

Percobaan Ke	Server	User yang digunakan	PC Client yang digunakan	Keterangan	Berhasil / Tidak Berhasil
1	Hotspot1	Fernaldo	PC Client 1	Sebelum di Konfigurasi	Berhasil
2	Hotspot1	Aldo	PC Client 1	Sebelum di Konfigurasi	Berhasil
3	Hs-Wlan1	Fernaldo	PC Client 2	Sebelum di Konfigurasi	Berhasil
4	Hs-Wlan1	Aldo	PC Client 2	Sebelum di Konfigurasi	Berhasil
5	Hotspot1	Fernaldo	PC Client 1	Setelah di Konfigurasi	Berhasil
6	Hotspot1	Aldo	PC Client 1	Setelah di Konfigurasi	Tidak Berhasil
7	Hs-Wlan1	Fernaldo	PC Client 2	Setelah di Konfigurasi	Tidak Berhasil
8	Hs-Wlan1	Aldo	PC Client 2	Setelah di Konfigurasi	Berhasil

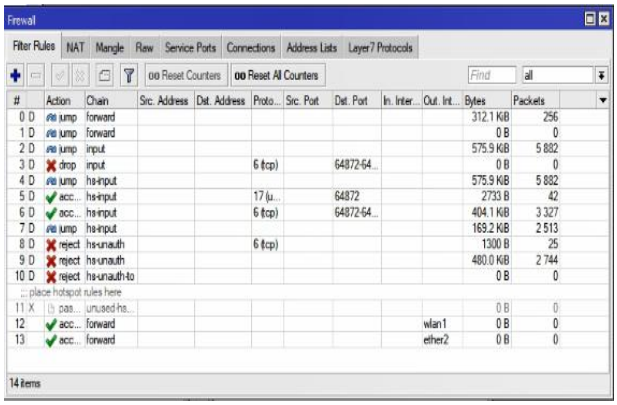
Pembahasan :

1. Uji coba 1 dan 2 dengan menggunakan PC *Client* 1, *user* Fernaldo dan Aldo berhasil dikarenakan *user profile* sudah didaftarkan.
2. Uji coba 3 dan 4 dengan menggunakan PC *Client* 2, *user* Fernaldo dan Aldo berhasil dikarenakan *user profile* sudah didaftarkan dikarenakan belum menambahkan *setting*-an firewall sehingga *user* tersebut dapat *login* ke semua PC *Client*.
3. Uji coba 5 dan 6 dengan menggunakan *user* Fernaldo Berhasil dan *user* Aldo Tidak Berhasil Login dikarenakan telah menambahkan *setting*-an *firewall* MAC-*Address Filter*, dan *user* Aldo tidak dapat *login* di PC *Client1* dikarenakan MAC *Address-nya* tidak sama dengan PC *Client1*.
4. Uji coba 7 dan 8 dengan menggunakan *user* Fernaldo Tidak Berhasil dan *user* Aldo Berhasil Login dikarenakan telah menambahkan *setting*-an *firewall* MAC-*Address Filter*, dan *user* Fernaldo tidak dapat *login* di PC *Client2* dikarenakan MAC *Address-nya* tidak sama dengan PC *Client2*.

Fitur *firewall* yang berupa keamanan NAT dan keamanan *filter rules* ini biasanya banyak digunakan untuk menandai koneksi maupun paket dari trafik data yang melewati *router*. Supaya fungsi dari fitur *firewall* dapat berjalan dengan baik, kita harus menambahkan rule-rule yang sesuai seperti pada Gambar 4.3 dan Gambar 4.4.



Gambar 4.3 Keamanan pada NAT



Gambar 4.5.Kemanan Pada Filter Rules

4. KESIMPULAN

Dengan adanya aplikasi keamanan data *user* berbasis web ini memudahkan operator jaringan untuk mendaftarkan MAC *Address* mahasiswa dan pengguna *wireless* di jurusan Teknik Komputer.

Sistem keamanan internet menggunakan *firewall* yaitu dengan cara melakukan *setting* pada *filter rules* dan NAT membantu pengguna untuk meminimalisir terjadinya penyalahgunaan hak akses jaringan wireless di jurusan Teknik Komputer.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Pimpinan manajemen Politeknik Negeri Sriwijaya yang memberikan dana penelitian terhadap pelaksanaan kegiatan ini.

DAFTAR PUSTAKA

[1] M. V. Pawar and J. Anuradha, "Network security and types of attacks in network," *Procedia Comput. Sci.*, vol. 48, no. C, pp. 503–506, 2015, doi: 10.1016/j.procs.2015.04.126.

[2] G. P. Gupta and M. Kulariya, "A Framework for Fast and Efficient Cyber Security Network Intrusion Detection Using Apache Spark," *Procedia Comput. Sci.*, vol. 93, no. September, pp. 824–831, 2016, doi: 10.1016/j.procs.2016.07.238.

[3] M. F. Duskarnaen and F. Nurfalah, "Analisis, Perancangan, Dan Implementasi Jaringan Wireless Point To Point Antara Kampus A Dan Kampus B Universitas Negeri Jakarta," *PINTER J. Pendidik. Tek. Inform. dan Komput.*, vol. 1, no. 2, pp. 134–141, 2017, doi: 10.21009/pinter.1.2.6.

[4] J. M. Sinambela, "Keamanan Wireless LAN (Wifi)," *Gadjahmada.Edu*, no. April, p. 5, 2007.

[5] Bhavya Daya, "Network security: History, importance, and future," *Univ. Florida Dep. Electr. ...*, p. 13, 2013, [Online]. Available: http://www.alphawireless.co.za/wp-content/uploads/2013/01/Network-Security-article.pdf.

[6] D. Angela, "Optimasi Jaringan Wireless LAN (Studi Kasus Di Kampus ITHB Bandung)," *J. ITHB*, vol. 6, no. 80, p. 8, 2010, [Online]. Available: https://journal.ithb.ac.id/telematika/article/view/39.

[7] R. Jjx, "ANALISIS PERBANDINGAN SISTEM KEAMANAN WEP / WPA / RADIUS PADA JARINGAN PUBLIK."

[8] D. M. Sari, M. Yamin, and L. B. Aksara, "Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration testing," *SemanTIK*, vol. 3, no. 2, pp. 203–208, 2017, doi: 10.1016/j.neuropharm.2007.08.010.

[9] H. I. Bulbul, I. Batmaz, and M. Ozel, “Wireless network security: Comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) security protocols,” *e-Forensics 2008 - Proc. 1st Int. Conf. Forensic Appl. Tech. Telecommun. Information, Multimed. Work.*, no. Icv, pp. 1–6, 2008, doi: 10.4108/e-forensics.2008.2654.