Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 1-8
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Sniffing Pada Jaringan *WiFi* Berbasis Protokol 802.1x Menggunakan Aplikasi *Wireshark*

Muhamad Aznar Abdillah[1], Anton Yudhana[2], Abdul Fadil[3]
[1] Magister Teknik Informatika Universitas Ahmad Dahlan
[2,3] Program Studi Teknik Elektro, Universitas Ahmad Dahlan
Jl. Prof. Dr. Soepomo, S.H., Janturan, Warungbroto, Umbulharjo, Yogyakarta
[1]muhamadaznar@gmail.com, [2] eyudhana@ee.uad.ac.id, [3]fadil@mti.uad.ac.id

Abstract

Nowadays WiFi technology is increasing with the people's need for internet access. WiFi is an abbreviation of Wireless Fidelity. WiFi can be said to be a technology for exchanging data by utilizing radio waves (wireless) that can be used by several electronic devices such as computers, smartphones, tablets, and so on. This research tries sniffing method on WiFi-based 802.1X protocol to get the client authentication code. The conclusion obtained from this study is the Sniifing Process using the Wireshark application managed to get the station authentication code on an 802.1X-based WiFi network. The authentication code can be used when the station is no longer connected to a WiFi network. This can be used by other people or stations that are actually not entitled / illegitimate.

Keywords*: Sniffing, Protokol 802.1X, Wireshark*

Abstrak

Dewasa ini teknologi WiFi semakin meningkat seiring kebutuhan masyarakat terhadap akses internet. WiFi merupakan singkatan dari Wireless Fidelity. WiFi dapat dikatakan sebuah teknologi untuk saling bertukar data dengan memanfaatkan gelombang radio (nirkabel) yang dapat digunakan oleh beberapa perangkat elektronik seperti computer, smartphone, tablet, dan sebagainya. Penelitian ini mencoba metode sniffing pada WiFi berbasis protokol 802.1X untuk mendapatkan kode otentikasi client. Kesimpulan yang diperoleh dari penelitian ini adalah Proses Sniifing dengan menggunakan aplikasi Wireshark berhasil mendapatkan kode otentikasi station pada jaringan WiFi berbasis 802.1X. Kode otentikasi dapat digunakan pada saat station tersebut sudah tidak terhubung dengan jaringan WiFi. Hal ini dapat dimanfaat oleh orang lain atau station yang sebenarnya tidak berhak / tidak sah.

Kata kunci*: Sniifing, Protokol 802.1X, Wireshark*

1. PENDAHULUAN

Dewasa ini teknologi *WiFi* semakin meningkat seiring kebutuhan masyarakat terhadap akses internet. *WiFi* merupakan singkatan dari *Wireless Fidelity*. *WiFi* dapat dikatakan sebuah teknologi untuk saling bertukar data dengan memanfaatkan gelombang radio (nirkabel) yang dapat digunakan oleh beberapa perangkat elektronik seperti komputer, *smartphone*, tablet, dan sebagainya [1]. *WiFi* memiliiki berbagai kelebihan yang menjadikan teknologi ini menjadi primadona bagi masyarakat. Pada jaringan komputer dikenal istilah protokol, yaitu sekumpulan aturan / prosedur atau standar yang digunakan untuk mengirimkan data antara perangkat elektronik. Protokol mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih computer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya [2].

Beberapa kelebihan *WiFi* diantaranya adalah bahwa teknologi ini lebih fleksibel atau pengguna bisa berpindah tempat, jaringan internet dapat diakses lebih mudah, juga penggunaan listrik yang lebih efisien. Namun dengan kelebihan yang dimiliki teknologi ini tak dapat dihindari kekurangan yang ada, seperti jaringan yang kurang aman dan bisa di sadap, perangkat yang cukup mahal, kualitas sinyal yang tidak baik pada kondisi tertentu. Hal ini sesuai dengan pendapat bahwa kemudahan mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Keamanan jaringan menjadi hal yang menarik untuk dibahas mengingat hal diatas. Kemanan jaringan penting dilakukan oleh administrator jaringan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Keamanan jaringan komputer (*computer network security*) harus menjadi perhatian yang besar pada saat kita akan membangun sebuah infrastruktur jaringan [3].

Optimasi jaringan LAN menggunakan VLAN memang dapat membuat jaringan akan lebih aman dan memiliki *security* yang tinggi [4], namun VLAN akan mendapatkan kendala ketika diterapkan pada jaringan Nirkabel (*WiFi*) karena tidak semua perangkan *WiFi* support VLAN dan pada pembahasan kali ini penulis fokus pada keamanan protokol 802.1X. Pada jaringan nirkabel (*WiFi*) dikenal Protokol 802.1x yang memiliki tingkat keamanan yang dianggap paling baik dan paling canggih. Protokol ini biasanya digunakan pada jaringan berbasis enterprise & bukan untuk jaringan berbasis rumah atau swasta. Protokol 802.1x menggunakan server otentikasi untuk mengotentikasi koneksi antara *access point* dan *station*. Komunikasi antara *access point* dan *authentication server* diimplementasikan menggunakan protokol yang berbeda. Adanya protokol 802.1X mensyaratkan validasi oleh *authenticator* sebelum *client* dapat benar-benar terhubung ke internet. Validasi yang dimaksud adalah *username* dan *password* bagi station yang akan terhubung ke internet, sehingga username yang tidak berhak / tidak sah tidak akan dapat menikmati internet dari *WiFi* berbasis protokol ini. Jenis topologi dimana setiap *client* dihubungkan secara langsung ke *server* atau *switch/hub* disebut sebagai tolopogi bintang (*star*). Topologi ini tahan terhadap lalu lintas yang tinggi namun sangat bergantung kepada fungsionalitas *hub* pusat [5]. Pada jaringan LAN nirkabel (*WiFi*) dapat dikatakan menggunakan topologi jenis *star* ini. Penelitian ini mencoba metode *sniffing* pada *WiFi* berbasis protokol 802.1X untuk mendapatkan kode otentikasi *client*. Setelah kode otentikasi didapatkan maka akan dapat digunakan untuk menghubungkan perangkat kita ke *WiFi* tersebut.

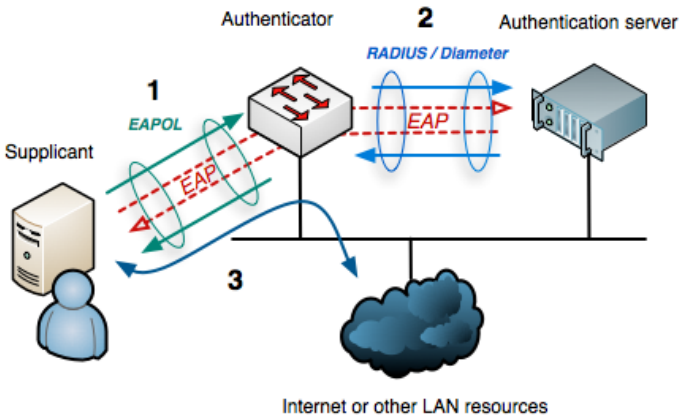
2. METODOLOGI PENELITIAN

Penelitian ini mencoba melakukan metode *sniffing* pada jaringan *WiFi* yang berbasis protokol 802.1X untuk mendapatkan hasil *capture traffic* dan mendapatkan *username* dan *password* sebuah *station*. Aplikasi yang digunakan pada proses *sniffing* adalah *Wireshark*. Peralatan dan bahan yang digunakan pada penelitian ini diantaranya sebagai berikut:

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 1-8
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

1. Modem, sebagai sumber internet
2. Mikrotik RB941-2nD-TC, sebagai *authentication server*
3. Acces Point NSM2 Loco
4. Laptop HP, sebagai *station* / pengguna
5. Aplikasi *Wireshark*

Adapun topologi protokol 802.1X sebagai berikut :



Gambar 1. Topologi protokol 801.2X

Aplikasi *Wireshark* bertugas untuk melakukan proses *capturing traffic* data saat sebuah station melakukan proses meminta autentikasi. Hasil capture tersebut selanjutnya dilakukan analisa untuk mendapatkan kode otentikasi *station* tersebut.

3. HASIL DAN PEMBAHASAN

Proses awal penelitian ini adalah membangun jaringan *WiFi* berbasis protokol 802.1X. Setelah jaringan *WiFi* terbentuk dan di uji coba selanjutnya menginstall aplikasi *Wireshark* untuk kemudian di gunakan untuk melakukan proses capturing traffic internet yang berlangsung. Setelah station meminta otentikasi dan memastikan dapat menikmati layanan internet lalu hasil capture traffic yang di dapatkan dilakukan analisa untuk mencari kode otentikasi yang berupa username dan password station.

3.1. Membangun *WiFi* 802.1X

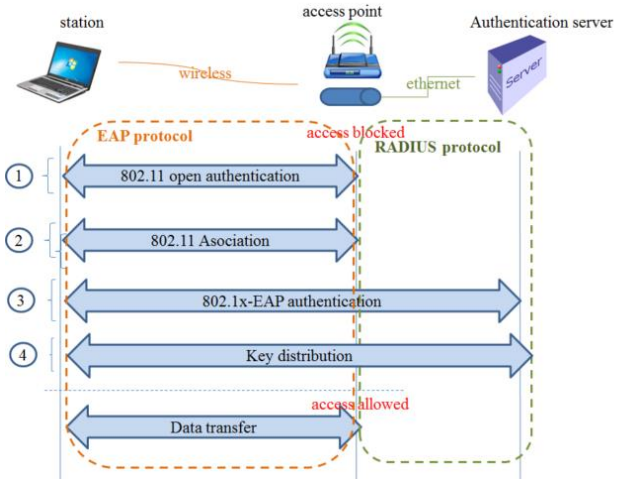
Metode otentikasi 802.1X lebih canggih dibanding WPA / WPA2 (*WiFi* Protected Access). Hal yang berbeda dengan WPA / WPA2 adalah metode otentikasi ini juga melibatkan pihak lain, yaitu server otentikasi untuk mengotentikasi koneksi antara access point dan station [5]. Implementasi otentikasi 802.1X mencakup 4 langkah sebagai berikut :

1. Sebuah stasiun dan jalur melakukan otentikasi sistem terbuka seperti yang didefinisikan oleh standar IEEE 802.11
2. Sebuah stasiun dan jalur akses melakukan hubungan normal seperti yang didefinisikan oleh standar IEEE 802.11

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 1-8
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

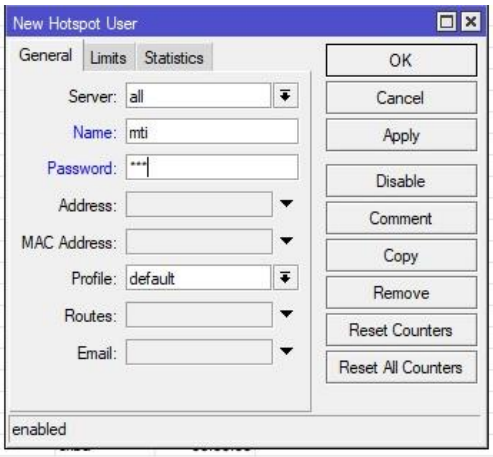
3. Otentikasi 802.1X dilakukan antara server otentikasi dan stasiun dengan access point sebagai mediator. Di akhir proses ini, sebuah stasiun diautentikasi oleh server otentikasi
4. Distribusi kunci akan dilakukan antara access point dan stasiun. Pada langkah ini, jalur akses dan stasiun menghasilkan kunci bersama dan saling mengotentikasi

Setelah jalur akses dan stasiun mengotentikasi satu sama lain, maka stasiun bisa mulai mengakses jaringan. Karena memerlukan server otentikasi dalam pelaksanaanya, metode ini biasa di terapkan di jaringan berbasis enterprise. Ilustrasi lengkap otentikasi 802.1X ditunjukan pada gambar berikut :



Gambar 2. Ilustrasi otentikasi 802.1X

Adapun kode otentikasi yang telah dibuat pada penelitian ini untuk digunakan oleh sebuah station agar dapat mendapatkan koneksi (username : mti, password : uad) seperti yang ditampilkan dalam gambar berikut:

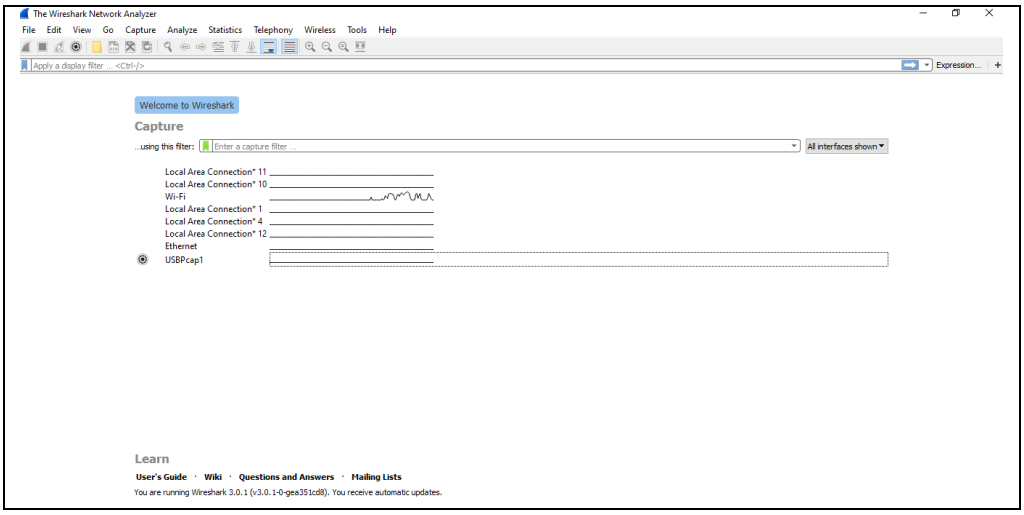


Gambar 3. Pembuatan sebuah kode otentikasi

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 1-8
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

3.2. *Wireshark*

Wireshark adalah sebuah *Network Packet Analyzer*. *Network Packet Analyzer* akan mencoba menangkap paket-paket jaringan dan berusaha unutk menampilkan semua informasi di pakey tersebut sedetail mungkin [6]. *Wireshark* dapat menganalisis paket data secara real time. Artinya aplikasi *Wireshark* ini akan mengawasi semua paket data yang keluar masuk melalui antar muka yang telah di tentukan oleh user sebelumnya untuk kemudian menampilkannya [7]. *Wireshark* dapat diunduh dari web secara gratis untuk selanjutnya dilakukan instalasi pada perangkat laptop / computer dan menjalankannya. Berikut adalah gambar antar muka aplikasi *Wireshark* yang telah berhasil di install :



Gambar 4. Antar muka aplikasi *Wireshark*

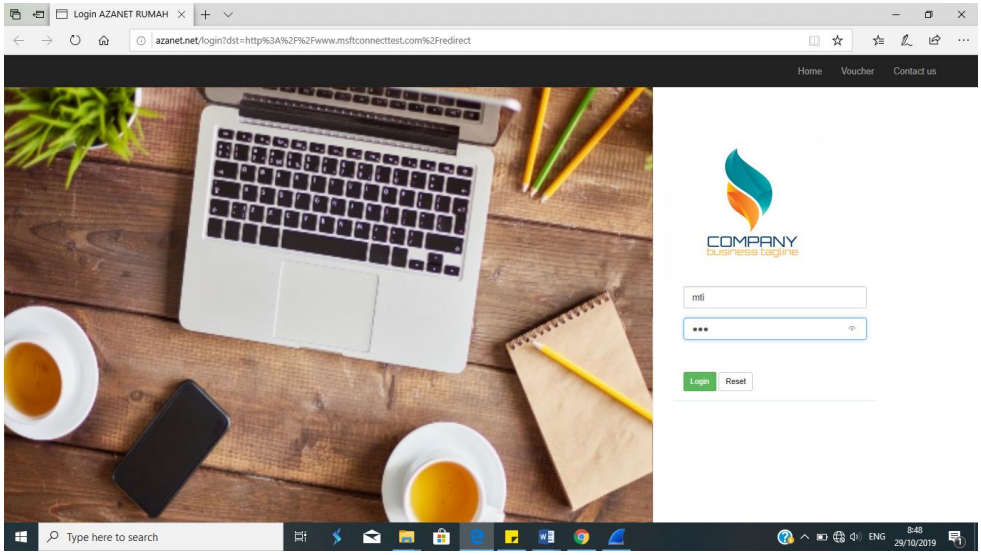
Saat aplikasi *Wireshark* di jalankan, akan tampak interface yang tersedia, berikut interface yang sedang bekerja dengan penanda terdapat traffic berupa grafik pada interface yang berjalan.

3.3. Proses Sniffing dan Analisis Hasil Capture

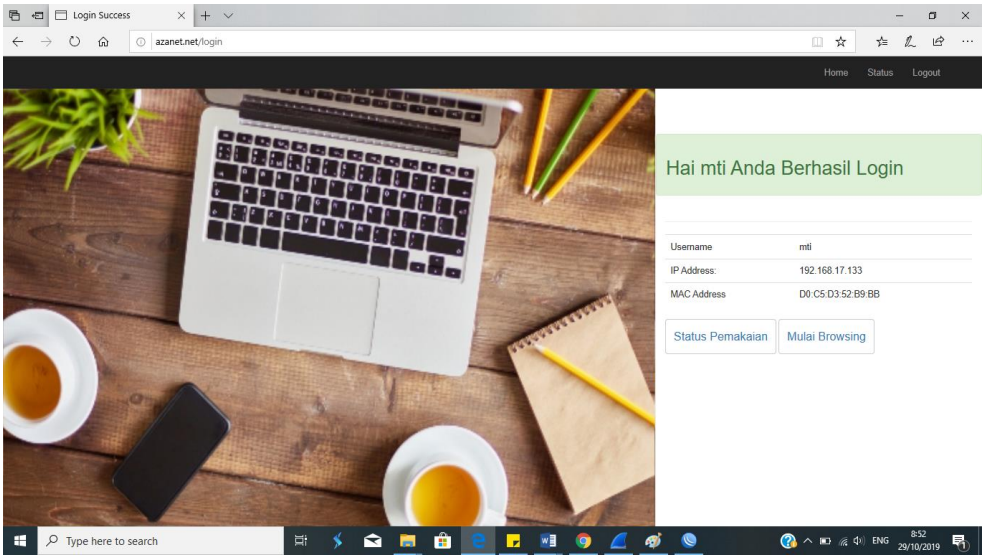
Aplikasi *Wireshark* yang telah di install dalam laptop di jalankan (*running*) dengan klik dua kali pada interface *WiFi*, karena pada penelitian ini fokus pada jaringan nirkabel / *WiFi*. Selanjutnya berperan sebagai seorang user yang akan menikmati koneksi internet dengan kode otentikasi yang telah dibuat sebelumnya. Setelah berhasil login dan mencoba / memastikan koneksi internet dapat dinikmati, proses *capturing Wireshark* dihentikan untuk kemudian hasil *capture traffic* tersebut di simpan dan dianalisis, apakah kode otentikasi yang berupa *username* dan *password* user tersebut dapat tertangkap di file hasil *capturing Wireshark*.

Berikut adalah gambar proses login sebuah station pada jaringan *WiFi* berbasis 802.1X:

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 1-8
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti



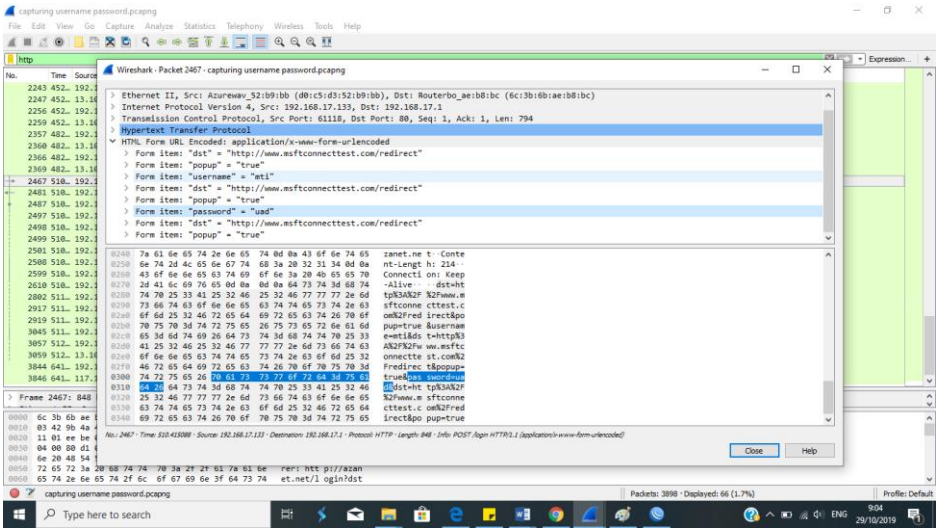
Gambar 5. Proses login sebuah station pada *WiFi* berbasis 802.1X



Gambar 6. Proses Login berhasil

Selanjutnya hasil *capture traffic* data pada *Wireshark* diakhiri dan di simpan untuk dianalisis. Hasil analisis yang dilakukan diperoleh bukti bahwa kode otentikasi yang berupa username dan password pada jaringan *WiFi* berbasis protocol 802.1X berhasil di peroleh seperti ditunjukan pada gambar berikut :

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 1 Maret 2020, pp. 1-8
ISSN: 2548-9771/EISSN: 2549-7200
http://tunasbangsa.ac.id/ejurnal/index.php/jsakti



Gambar 7. Hasil analisa dan pencarian kode otentikasi

Pada paket ke 2467 dalam hasil capturing *Wireshark* yang telah dilakukan terdapat kode otentikasi yang digunakan untuk menikmati koneksi internet pada station. Terlihat pada baris yang menunjukan kode tersebut, ada pada baris 'HTML Form URL Encoded'. Penelitian ini menunjukan bahwa *Wireshark* mampu menangkap kode otentikasi yang berupa username dan password pada jaringan *WiFi* berbasis protocol 802.1X sehingga pengguna jarring 802.1X sekalipun harus tetap berhati-hati dan bijak dalam menggunakan layanan internet.

4. SIMPULAN

Kesimpulan yang diperoleh dari penelitian ini adalah Proses Sniifing dengan menggunakan aplikasi *Wireshark* berhasil mendapatkan kode otentikasi station pada jaringan *WiFi* berbasis 802.1X. Kode otentikasi dapat digunakan pada saat station tersebut sudah tidak terhubung dengan jaringan *WiFi*. Hal ini dapat dimanfaat oleh orang lain atau station yang sebenarnya tidak berhak/ tidak sah. Pada penelitian berikutnya dapat dilanjutkan untuk mencoba masuk/ *login* pada sistem authentication server pada sebuah jaringan *WiFi* berbasis 802.1X. Apabila penelitian tersebut berhasil dapat dilanjutkan dengan melanjutkan penelitian mengenai cara pencegahan serangan tersebut agar penelitian ini dapat dirasakan manfaatnya bagi administrator jaringan.

DAFTAR PUSTAKA

[1] Tonapa, O., Pauline R., Debora K., "Analisis Performansi Konektifitas Pada Jaringan Wireless Broadband di Bandung", Jurnal ELKOMIKA Institut Teknologi Nasional Bandung, Vol. 2, No. 2, Juli – Desember 2014.

[2] Primartha, R., "Manajemen Jaringan Komputer", Penerbit INFORMATIKA, Bandung, 2019.

[3] Sugiyono, "Sistem Keamanan Jaringan Komputer Menggunakan Metode Watchguard Firebox pada PT Guna Karya Indonesia", Jurnal CKI On SPOT, Vol. 9, No.1, Juni 2016.
[4] Wahyu, A.P., "Optimasi Jaringan Local Area Network Menggunakan VLAN dan VOIP", Jurnal Informatika:Jurnal Pengembangan IT, Vol.2, No.1, Januari 2017.
[5] Rofii, F., Fachrudin H., Shofie S., "Kinerja Jaringan Komunikasi Nirkable Berbasis Xbee pada Topologi Bus, Star dan Mesh", ELKOMIKA Vol. 6, No. 3, Halaman 393-404, September 2018.
[6] Surantha, N., "IEEE 802.1X-EAP Untuk Jaringan Berbasis Enterprise", https://mti.binus.ac.id/2017/06/08/ieee-802-1x-eap-untuk-jaringan-berbasis-enterprise/, di unduh 28 Oktober 2019 22.00 WIB.
[7] Khairina, D. M., "Analisis Keamanan Sistem Login", Jurnal Informatika Mulawarman Vol.6, No.2, Halaman 64 – 67, Juli 2011.
[8] Diansyah, T.M., "Analisa Pencegahan Aktivitas Illegal di Dalam Jaringan Menggunakan *Wireshark*", Jurnal TIMES, Vol. IV, No. 2 : 20-23, 2015