Analisis Keamanan Jaringan Pada Layanan Wifi Dengan Menggunakan Wireshark

[1]Ariel Teza Permana, [2]Albi Fajar Ramadhan
[1,2] Fakultas Teknologi Informasi, Universitas Sebelas April Sumedang
[1,2] Jl Angkrek Situ No 19 Kab Sumedang, Jawa Barat, Indonesia
[1]a2.2000011@mhs.stmik-sumedang.ac.id, [2]Albi Fajar@gmail.com

ABSTRACT
WiFi is an acronym for Wireless Fidelity. WiFi can be said to be a technology for exchanging data by utilizing radio waves (wireless) which can be used by several electronic devices such as computers, smartphones, tablets, and so on. WiFi has various advantages that make this technology a prima donna for the community. In computer networks, the term protocol is known, which is a set of rules/procedures or standards used to transmit data between electronic devices. Currently, information security issues are becoming important, especially the process of tapping information (sniffing) on computer networks is becoming increasingly common, both for positive and reverse uses. In this study, the sniffing process was used to obtain username and password information. The sniffing process is done using the Wireshark software. Wireshark is a software application that is used to view and analyze data packets passing on a network. Wireshark is a network packet analysis program that will capture network packets and try to display data from a packet as detailed as possible. The Wireshark software performs the process of capturing data on the Wireless interface, then observes the captured results which contain POST data containing username and password on HTTP. From the results of the research conducted, it was found that using Wireshark can intercept data carried out on computer networks, this results in the loss of one of the security characteristics, namely privacy and confidentiality.

Keywords **-** analysis, network security on wifi services, wireshark

ABSTRAK
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 . 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. Saat ini permasalahan keamanan informasi menjadi penting, khususnya proses penyadapan informasi (Sniffing) pada jaringan komputer menjadi semakin biasa dilakukan, baik untuk kegunaan yang bersifat positif maupun yang bersifat sebaliknya. Dalam penelitian ini, proses sniffing digunakan untuk mendapatkan informasi username dan password. Proses sniffing dilakukan menggunakan perangkat lunak Wireshark. Wireshark merupakan aplikasi perangkat lunak (software) yang digunakan untuk melihat dan menganalisa paket-paket data yang lewat pada jaringan. Wireshark merupakan sebuah program analisa paket jaringan yang akan menangkap paket jaringan dan mencoba untuk menampilkan data dari sebuah paket yang sedetail mungkin. Software Wireshark melakukan proses capturing data pada interface Wireless, lalu mengamati hasil capture-an yang berisikan data POST yang berisi username dan password pada HTTP. Dari hasil penelitian yang dilakukan didapatkan bahwa dengan menggunakan Wireshark dapat melakukan penyadapan data yang dilakukan pada jaringan komputer, hal ini mengakibatkan hilangnya salah satu sifat keamanan yaitu privacy dan confidentiality.

Kata Kunci **-** analisis, keamanan jaringan pada layanan wifi, wireshark

1. Pendahuluan

Perkembangan teknologi informasi dalam jaringan komputer berkembang sangat pesat dan fleksibel. Internet merupakan jaringan komputer yang digunakan karena kemudahan aksesnya. 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 . 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 komputer. Protokol dapat diterapkan pada perangkat keras, perangkat lunak atau kombinasi dari keduanya. [1]

Seiring dengan pesatnya perkembangan teknologi tersebut, semakin besar pula ancaman dan gangguan terhadap kinerja dalam teknologi tersebut. Untuk itu keamanan jaringan merupakan aspek penting yang harus diperhatikan. Keamanan jaringan komputer kini dipandang sebagai salah satu tugas dan masalah penting yang harus dibenahi, solusinya untuk melindungi aset-aset dan berbagai informasi. Keamanan jaringan adalah proses pencegahan yang dilakukan oleh penyerang untuk terhubung ke dalam jaringan komputer melalui akses yang tidak sah atau penggunaan secara ilegal dari komputer dan jaringan. Faktor-faktor penyebab resiko jaringan komputer meliputi kelemahan manusia, kelemahan perangkat keras komputer, kelemahan sistem operasi jaringan dan kelemahan sistem jaringan komunikasi.[2]

Salah satu teknik dalam mempertahankan keamanan adalah menggunakan Wireshark. Wireshark merupakan aplikasi perangkat lunak (software) yang digunakan untuk melihat dan menganalisa paket-paket data yang lewat pada jaringan. Wireshark merupakan sebuah program analisa paket jaringan yang akan menangkap paket jaringan dan mencoba untuk menampilkan data dari sebuah paket yang sedetail mungkin. Sangat mudah dipakai karena menggunakan wireshark. Semakin berkembangnya teknologi informasi sekarang ini, maka kebutuhan akan informasi semakin meningkat pula, dimana setiap orang membutuhkan informasi dalam waktu yang cepat, singkat dan akurat oleh karena itu dibutuhkan suatu sarana yang mendukung hal tersebut.[3]

2. Metodologi

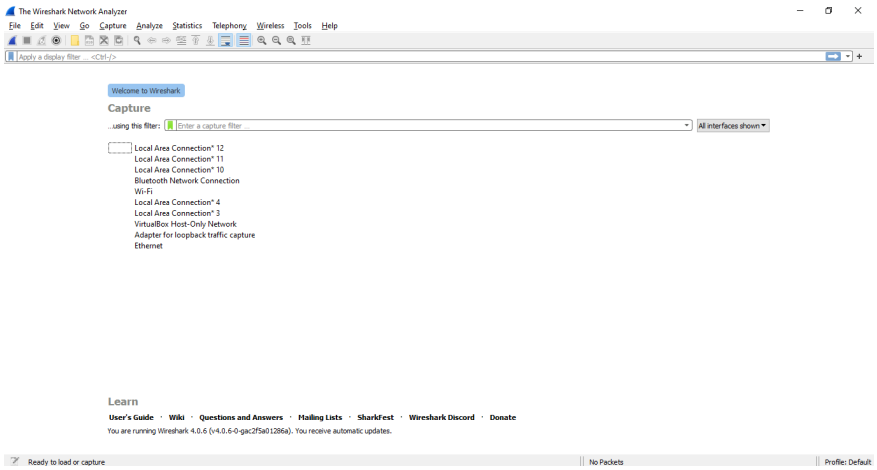
Penelitian ini mencoba melakukan metode sniffing pada jaringan WiFi yang berbasis protokol untuk mendapatkan hasil capture traffic dan mendapatkan username dan password sebuah station. Aplikasi yang digunakan pada proses sniffing adalah Wireshark.

3. Hasil dan Pembahasan

Berikut langkah-langkah untuk menggunakan wireshark di website :

1. Jalankan Wireshark

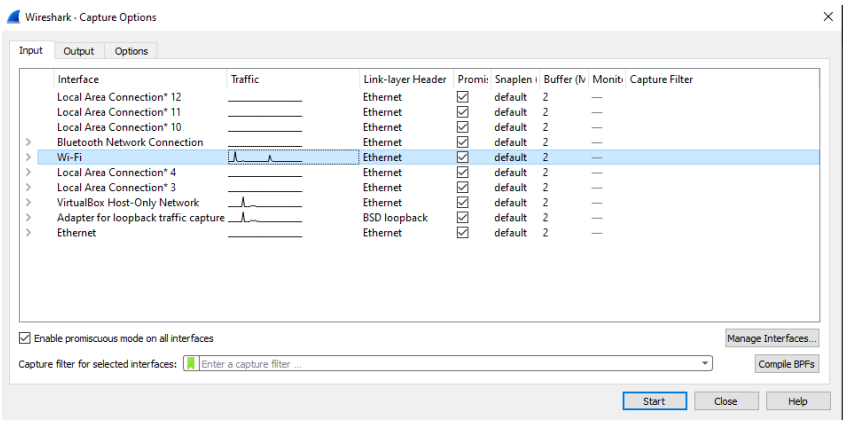
   Memantau akses browser yang dijalankan menggunakan wireshark dan mencoba memonitor jaringan Wi-Fi, seperti pada gambar dibawah ini.



Gambar 1. *Tampilan Wireshark*

2. Memilih interface yang akan dimonitor

Memilih capture yang akan dimonitor, lalu pilih WiFi setelah itu tekan start, seperti gambar dibawah ini.



Gambar 2. *Memilih Capture*

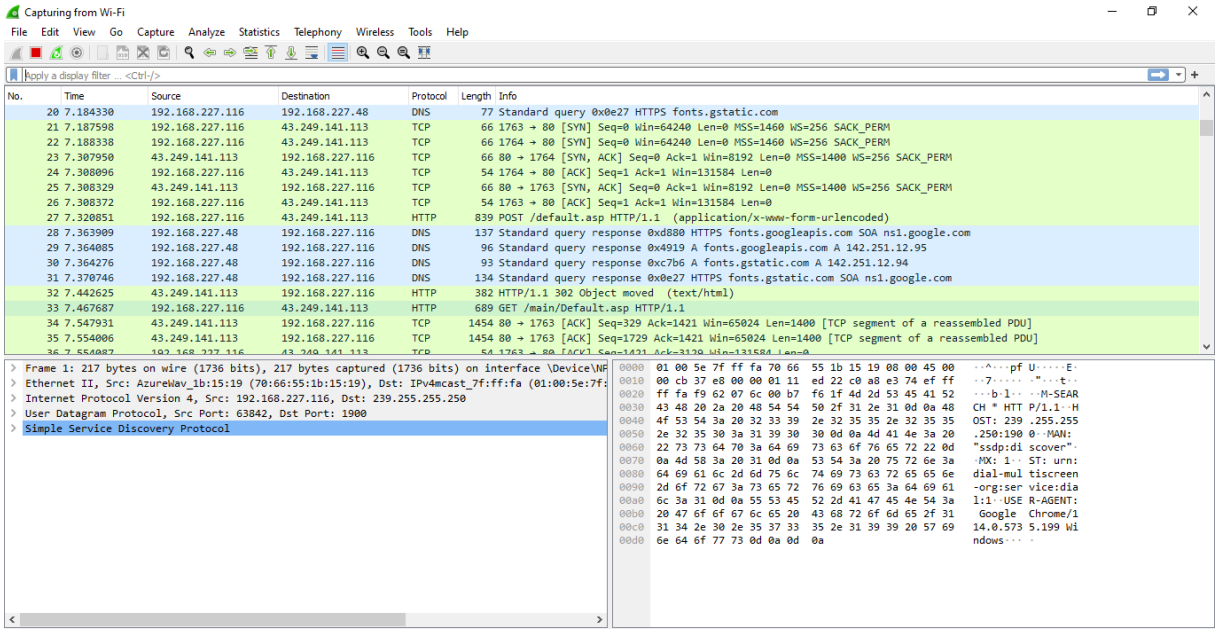
3. Membuka website, lalu masukan username dan password.

Gambar 3. *Membuka SIAP STMIK Sumedang*

Dari tampilan diatas, program wireshark dijalankan lalu memilih interface service networks, lalu memilih interface WiFi lalu klik start, setelah itu membuka web SIAP STMIK Sumedang dan masukkan username dan password lalu log in.

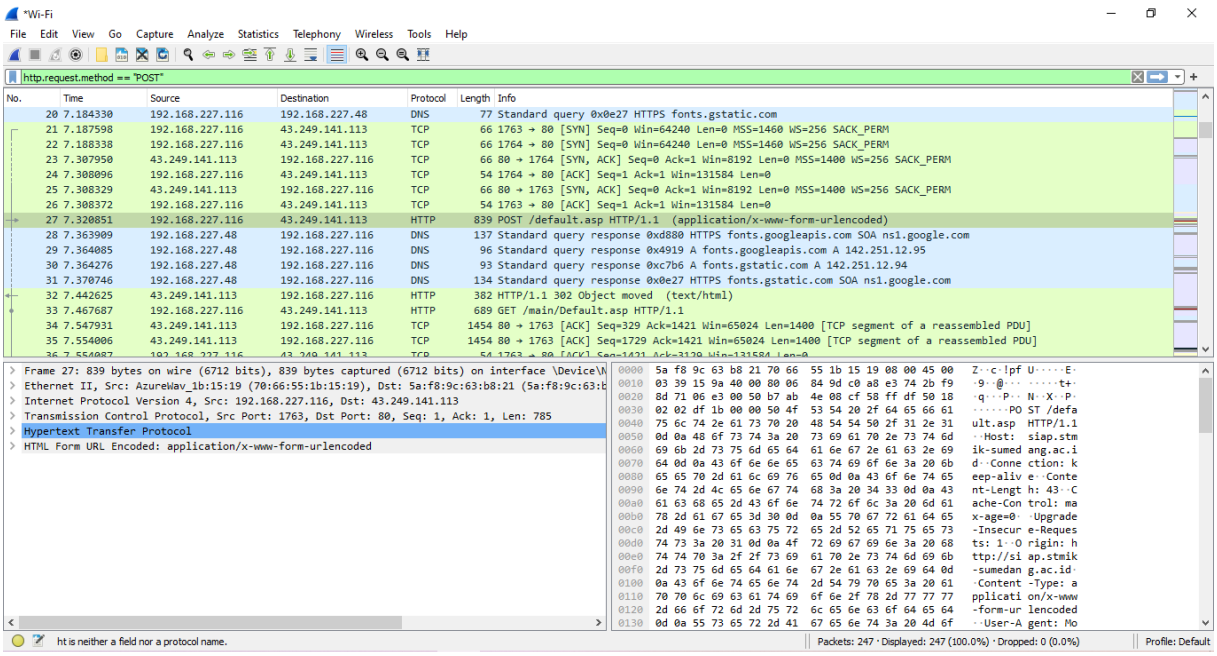
Pembahasan

Dari hasil percobaan diatas mendapatkan hasil capture seperti dibawah ini.



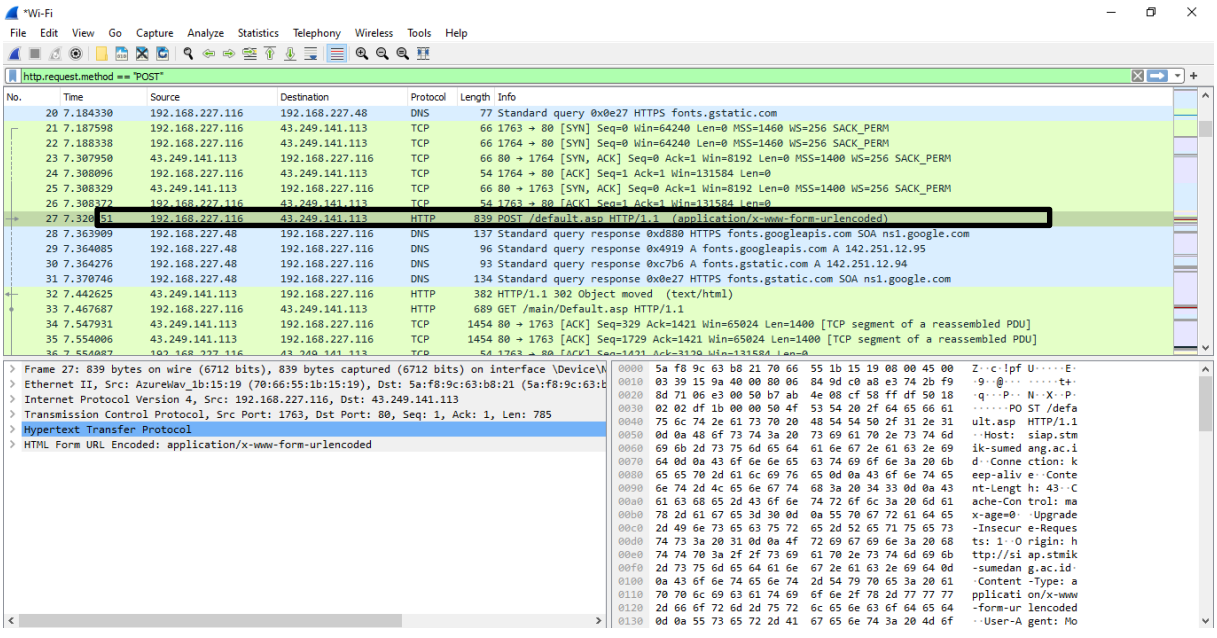
Gambar 4. *Hasil Capture*

1) Hasil capture-an seperti pada gambar diatas belum dilakukan pemfilteran, sehingga semua data yang lewat pada jaringan tersebut direkam sehingga menyulitkan untuk dilakukan analisa. Setelah itu, akan melakukan pemfilteran dengan memilih protokol HTTP seperti yang ditunjukkan pada gambar 5 dibawah ini.



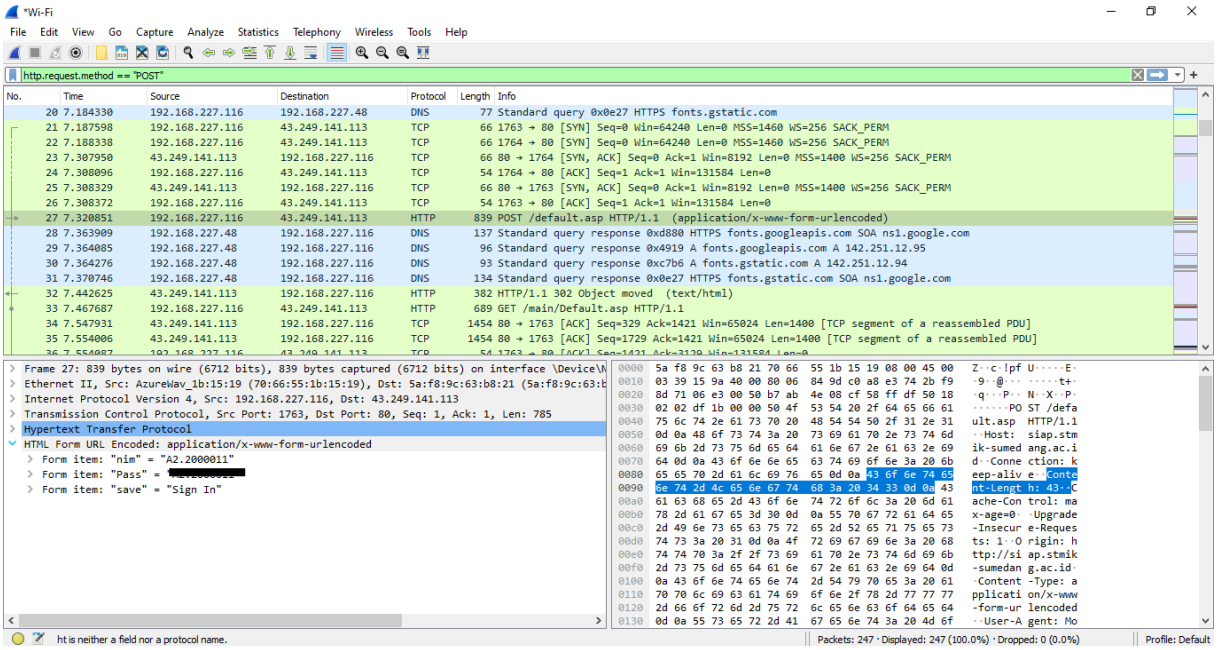
Gambar 5. *Filteran Paket HTTP*

2) Setelah melakukan capture pada protokol HTTP, selanjutnya lakukan analisa pada paket yang berisikan data POST seperti pada gambar 6 dibawah ini.



Gambar 6. *Paket yang Berisi Data POST*

3) Pada data POST ada beberapa informasi seperti, alamat IP 192.168.227.116 source dan 43.249.141.113 destination, lalu terdapat HTTP yang berisi POST, bos, connection, content-lenght, origin, user-agent, dan yang paling penting HTML for URL yang berisi username dan password seperti gambar 7 dibawah ini.



Gambar 7. *Hypertex transfer protokol*

4) Sniffing username dan password menggunakan Wireshark berhasil. Dengan hasil capture yang di analisa melalui jaringan pada jaringan terpilih bisa diketahui username dan password pada paket data POST.

4. Kesimpulan

Dengan menggunakan wireshark memudahkan proses capture paket data secara langsung dari sebuah network interface, mampu menampilkan informasi yang sangat detail mengenai hasil informasi penting dan rahasia seperti username dan password. Dari percobaan diatas, sniffing merupakan suatu yang cukup sulit untuk dicegah. Untuk sekarang ini sudah ada beberapa cara pencegahan sniffing seperti menggunakan enkripsi pada data rahasia (username, password), HTTPS (Hypertex Transport Protocol Secure) pada PORT. Saran lebih ditunjukan pada asas kehati-hatian ketika melakukan aktivitas seperti mangakses halaman web email, e-banking, social media, pada jaringan internet yang belum dikenal walaupun itu menawarkan secara gratis.

Referensi

[1] J. Fernandes, “Analisis Keamanan Jaringan Wireles Landi Dinas Perpustakan Dan Kearsipan Kota Pekanbaru,” pp. 1–79, 2021.

[2] R. T. Novita, I. Gunawan, I. Marleni, O. G. Grasia, and M. N. Valentika, “Analisis Keamanan Wifi Menggunakan Wireshark,” *JES (J. Elektro Smart)*, vol. 1, no. 1, pp. 1–3, 2021.

[3] B. Sinuraya dan and Bremana Tarigan, “Sistem Monitoring Jaringan Wifi Menggunakan Wireshark Pada STMIK KNI Kristen Neumann Indonesia,” *Sist. Monit. Jar. Wifi Menggunakan Wireshark Pada STMIK KNI Kristen Neumann Indones.*, vol. 3, 2021.

[4] Firmansyah, E., Helmiawan, M. A., Fadil, I., Mahardika, F., Budiana, D., & Marliana, R. R. (2022, September). Integrated Academic Information System Based on The Perception of Ease And Benefits. In *2022 10th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-6). IEEE.

[5] DASMEN, Rahmat Novrianda, et al. Penerapan Keamanan Jaringan Menggunakan Metode Firewall Security Port: Network Security Implementation Using Firewall Security Port Method. *Decode: Jurnal Pendidikan Teknologi Informasi*, 2022, 2.1: 1-7.

[6] ILHAM, Karina Fitriwulandari Ilham; ALWI, Erick Irawadi; FATTAH, Farniwati. Penerapan dan Analisis Network Security Snort Menggunakan Intrusion Detection System pada Serangan UDP Flood. *INFORMAL: Informatics Journal*, 2023, 8.1: 94-100.

[7] ABDILLAH, Muhamad Aznar; YUDHANA, Anton; FADIL, Abdul. Sniffing Pada Jaringan WiFi Berbasis Protokol 802.1 x Menggunakan Aplikasi Wireshark. *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, 2020, 4.1: 1-8.

[8] LUTHFANSA, UDR Zaky Maula; ROSIANI, Ulla Delfana Unknown. Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet. *Journal Information Engineering and Educational Technology) ISSN*, 2021, 2549: 869X.

[9] Rospita, S., Firmansyah, E., & Helmiawan, M. A. (2024). Implementasi Google Family Link Sebagai Solusi Pengawasan Penggunaan Gadget Anak di Desa Sundamekar. *JIMT: Jurnal Informatika, Multimedia dan Teknik*, *1*(1), 83-88.

[10] RIZKYANI, RIZKYANI. *Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) Terhadap Serangan Packet Sniffing Di Kantor Koran Seruya*. Diss. UNIVERSITAS COKROAMINOTO PALOPO, 2019.

[11] UBAEDILA, Ibnu, et al. Layanan Jaringan Menggunakan Metode Sniffing Berbasis Wireshark. *INFORMATICS FOR EDUCATORS AND PROFESSIONAL: Journal of Informatics*, 2022, 6.1: 95-104.

[12] Mahmud, Putri Tsania. "Sniffing Jaringan Menggunakan Wireshark." (2020).

[13] Helmiawan, M. A., Fadil, I., Sofiyan, Y., & Firmansyah, E. (2021, September). Security model using intrusion detection system on cloud computing security management. In *2021 9th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-5). IEEE.

[14] Firmansyah, E., Helmiawan, M. A., Rahman, A., Supendi, P., Ningsih, S. B. H., Suhayati, M., & Rahman, A. A. (2021, April). Examining readiness of e-learning implementation using Aydin and Tasci model: A rural university case study in Indonesia. In AIP Conference Proceedings (Vol. 2331, No. 1). AIP Publishing.

[15] Helmiawan, M. A., Firmansyah, E., Fadil, I., Sofivan, Y., Mahardika, F., & Guntara, A. (2020, October). Analysis of web security using open web application security project 10. In 2020 8th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE.