OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 10, Oktober 2023
ISSN 2828-2442 (media online)
Hal 2593-2599

Monitoring Jaringan Internet Kantor Pusat Administrasi Universitas Muhammadiyah Palembang

Sayfudin[1*]

[1]Fakultas Teknik, Teknologi Informasi, Universitas Muhammadiyah Palembang, Palembang, Indonesia
Email: [1*]sayfudinbinsunarto@gmail.com
(* : coressponding author)

Abstrak− Pentingya internet dikehidupan sehari-hari membuat kehidupan manusia tidak bisa lepas dari internet namun tanpa disadari penggunaan internet terkadang dimanfaatkan pihak yang tidak bertanggung jawab untuk mencuri paket data melalui lalu lintas paket data yang ada di internet menggunakan metode sniifing dengna memanfaatkan *software open source* bernama wireshark, untuk itu perlu kita pahami bahwa penggunaan internet khususnya yang masih menggunakan protokol http. Ketika ingin mengakses *website* yang masih menggunakan *protocol http* disarankan untuk tidak menggunakna jaringan publik, karena pada penelitian ini telah membahas *protocol http* dapat memberikan data rahasia seperti *user* dan *password*, ini terjadi di kantor pusat administrasi Universitas Muhammadiyah Palembang dimana setelah dilakukan penelitian ada beberapa aplikasi yang masih menggunakan protocol http, tentunya ini membahayakan bagi pengguna. Untuk itu penelitian ini telah memberikan saran kepada UPT-IT selaku unit yang bertanggung jawab untuk segera mengugrade *protocol* dari http ke https agar pengguna internet dapat menggunakan internet tanpa takut data rahasia dicuri oeleh pihak yang tidak bertanggung jawab.

Kata Kunci: Monitoring Jaringan, Sniffing, Wireshark, Protocol Http

Abstract− *The importance of the internet in everyday life makes human life inseparable from the internet but without realizing it, the use of the internet is sometimes used by irresponsible parties to steal data packets through data packet traffic on the internet using the sniifing method by utilizing open source software called wireshark, for that we need to understand that the use of the internet, especially those that still use the http protocol. When you want to access a website that still uses the http protocol, it is advisable not to use a public network, because in this study it has discussed that the http protocol can provide confidential data such as users and passwords, this happened in the administrative center office of the University of Muhammadiyah Palembang where after research there were several applications that still used the http protocol, of course this was dangerous for users. For this reason, this research has provided advice to UPT-IT as the responsible unit to immediately upgrade the protocol from http to https so that internet users can use the internet without fear of confidential data being stolen by irresponsible parties.*

Keywords*: Netwok Monitoring, Sniffing, Wireshark, Http Protocol*

1. PENDAHULUAN

Internet merupakan infrastruktur penting yang digunakan diberbagai institusi pendidikan, termasuk universitas muhammadiyah palembang (umpalembang), yang saat ini sangat bergantung pada internet dalam menjalankan banyak aktivitasnya sehari-hari. Hal ini sejalan dengan hasil survey yang telah dilakukan oleh APJII bahwa penignkatan jumlah pengguna internet diberbagai bidang mengalami perkembangan pesat jika dibanding tahun lalu yaitu sebesar 215 juta pengguna, menigkat sebesar 2,67%(apjii, 2023).

Oleh karena itu salah satu aspek yang patut mendapat perhatian adalah pemantauan lalu lintas jaringan internet untuk memahami penggunaan dan potensi masalah yang mungkin timbul. Pentingnya pemantuan lalu lintas jaringan internet ini mendorong penelitian ini untuk fokus pada analisis lalu lintas jaringan internet di kantor pusat administrasi universitas muhammadiyah palembang.

Penelitian ini tidak dimaksudkan untuk mengembangkan sistem baru tetapi untuk mengekstrak informasi berharga menggunakan perangkat lunak *Wireshark* yang sudah ada. *Wireshark* adalah alat analisis protokol jaringan dan alat penangkap paket yang banyak digunakan dan bersifat *open source*(Bock, n.d.). Fokus utama penelitian ini adalah pada protokol *HTTP (Hypertext Transfer Protocol)* utamanya pada aplikasi berbasis web yang masih menggunakan protol *HTTP*. *Hypertext Transfer Protocol* merupakan sebuah protocol jaringan aplikasi yang digunakan untuk mendistribusikan informasi antara komputer *server* dengan *computer client* , *server* yang dimaksud ialah server web fisik dalam jaringan komputer dengan skala besar sedangkan *client*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 10, Oktober 2023
ISSN 2828-2442 (media online)
Hal 2593-2599

ialah *web browser* yang dapat mengkases, menerima dan menampilkan konten *web* melalui *browser*(Alfian Dharma Kusuma, 2020).

Pemahaman penyeluruh tentang protokol *HTTP* akan memberikan informasi yang diperlukan untuk mengoptimalkan kinerja jaringan, mengidentifikasi potensi ancaman keamanan, dan memastikan layanan yang stabil bagi pengguna. Dengan menggunakan teknologi pemantauan yang ada, penelitian ini akan menganalisis pola lalu lintas jaringna pada protocol *HTTP* yang terkait dengan aplikasi berbasis web di umpalembang yang sebagian masih menggunakan protocol *HTTP*.

Studi sebelumnya yang telah dilakukan Susianto D, Rachmawati A 2018 dengan judul *"Implementasi dan analisis jaringna menggunakan wireshark, chain and abels, network minner studi kasus amik dian cipta"* pada penelitian tersebut penggunaan wireshark dapat disimpulan bahwa wireshark merupakan alat yang sangat berguna dalam analisis dan pengamanan jaringan *WiFi*. *Wireshark* dapat digunakan untuk menangkap dan menganalisis paket data yang berada dalam jaringna *WiFi*, sehingga memungkinkan pengguna untuk melihat informasi sumber, tujuan protocol, dan waktu *capture* nya. Dengan menggunakan *wireshark* penelitian tersebut dapat memperoleh informasi yang diperlukan untuk informasi dan mengamankan jaringan *WiFi* (Susianto & Rachmawati, 2018).

Kemudian pada tahun 2020 Surahman M, dkk melakukan penelitian menggunakan *tools wireshark* untuk meng *capture* lalu lintas jaringan dengan judul *"Penerapan metode svm-based machine learning untuk menganalisa pengguna data trafik internet"* yang mana *tools wireshark* telah membantu mengumpulkan data lalu lintas jaringan kemudian data tersebut di klasifikasikan menggunakan *supervised vector machine(svm)* menggunakna *software weka* mendapati protocol yang banyak digunakan adalah protocol TCP (Surahman et al., 2020).

Selanjutnya pada tahun 2021 penelitian yang dilakukan F Huzaini, dkk dengan judul *"Analisis keamanan data pda website dengan wireshark"* menghasilkan kesimpulan bahwa penggunaan protocol *HTTP* pada *website* sangat berbahaya karena dapat menyebabkan kebocoran data pribadi seperti *username* dan *password* (Huzaeni et al., 2021) Masih ditahun yang sama Febriani Y, dkk dalam penelitianya yang berjudul *"Monitoring pencegahan aktivitas illegal dalam jaringan pada kantor dinas esdm sumatera selatan".* Penelitian tersebut menggunakna dua software untuk mengcapture lalulintas jaringan internet yaitu *wireshark* dan *network monitor* dari keduanya berhasil mendeteksi adanya serangan *sniffing* dan mencegah terjadinya kebocoran data (Febriani & Sahfitri, n.d.)

Terbaru penelitian yang dilakukan oleh Pchaudhary dkk tahun 2023 dengan penelitianya yang berjudul *"Network traffic analysis using wireshark"* dimana penelitian tersebut menggunakan *software wireshark* dalam melakukan capturing paket lalulintas jaringan dan penelitian ini menghasilkan pengembangna sebuah alat analisis jaringan yang dapat digunakan untuk memantau lalu lintas jaringan(Chaudhary et al., 2023)Dari semua penelitian yang telah dilakukan oleh peneliti terdahulu semakinmemantapkan peneliti untuk melakukan pemantauan lalu linta sinternet yang ada di kantor pusat administrasi universitas Muhammadiyah Palembang.

Penelitian ini akan memantau lalu lintas jaringan internet kemudian melakukan analisis hasil pemnatauan memberikan gambaran tentang bagaimana protokol *HTTP* digunakan di umpalembang, termasuk jumlah permintaan, metode otentikasi yang paling umum digunakan, dan pola *uptime*. Informasi ini dapat membantu administrator universitas mengambil langkah-langkah yang diperlukan untuk meningkatkan kinerja jaringan internet dan keamanan system.

Artikel dibuat kedalam halaman 1 kolom dengan ukuran kertas A4. Untuk Top Margin 4 cm, Left Margin 4 cm,

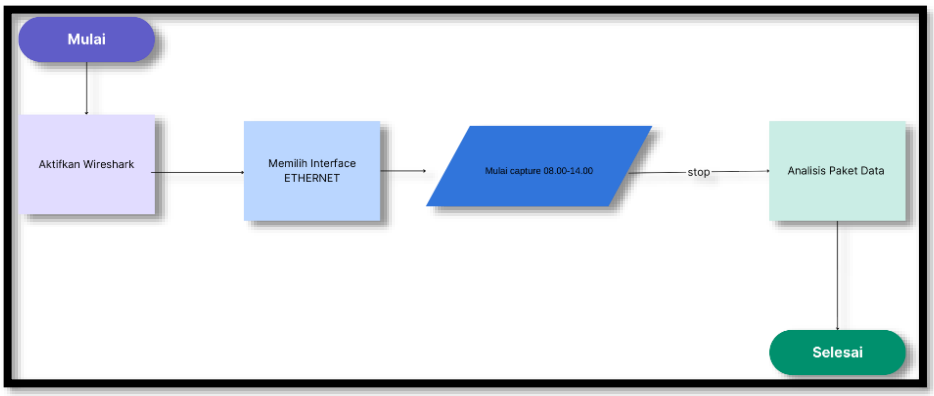
2. METODOLOGI PENELITIAN

Metode yang dilakukan dalam proses pemantauan lalu lintas jaringan dimulai dari pengumpulan data yang dikumpulkan melalui penangkapan paket data jaringan internet *LAN* (*Local Area Netrwork)* di kantor pusat adminsitrasi dengan menggunakan *software wireshark. LAN* (*Local Area Netrwork)* merupakan jaringan yang menghubungkan lebih dari satu computer yang mengkover area local, seperti rumah, kantor, atau grup dari bangunan(Nurdadyansyah & Hasibuan, n.d.). Data yang diambil ialah semua hasil pemantauan lalu lintas jaringan yang dilakukan di jam kerja, mulai dari jam 08.00-14.00 wib kemudian peneliti melakukan analisis data dan melakukan

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 10, Oktober 2023
ISSN 2828-2442 (media online)
Hal 2593-2599

filtering protocol, dalam hal ini data akan difilter berdasarkan protokol *HTPP*. Tahapan alur penelitian seperti yang tergambarkan pada gambar 1.

Proses pertama yang harus dilakukan ialah mengaktifkan *software wireshark* dengan memilih jaringan *LAN* (*Local Area Netrwork)*, pengaktifan dilakukan selama jam kerja memantau serta menunggu kemungkinan adanya akses aplikasi berbasis web yang dilakukan oleh karyawan, pastikan semua paket-paket internet tertangkap oleh *software wireshark*. Pada saat jam kerja telah selesai yaitu pukul 14.00 wib maka matikan atau *stop* proses pemantauan paket pada *wireshark*. Kemudian lakukan filtering menggunakna protocol *HTTP* dan temukan paket dengan *method POST* dan mulai menganalisa isi dari seluruh paket tersebut.



Gambar 1. Alur Penelitian

3. HASIL DAN PEMBAHASAN

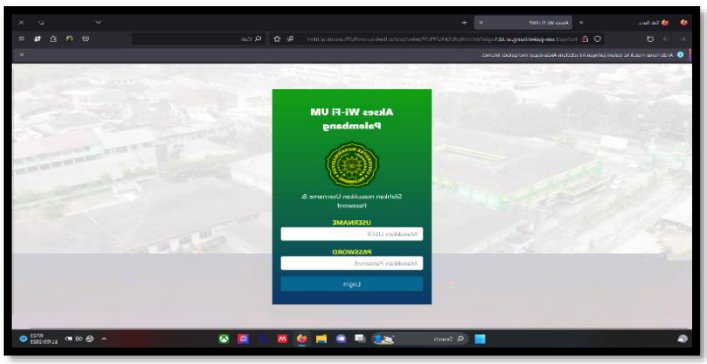
Penelitian telah dilakukan dengna mengikuti metode yang penulis buat dan saat pemantauan paket dihentikan peneliti mendapati paket data lalu lintas internet yang tercapture sebanyak 1.223.392 paket, namun setelah dilakukan filtering ke protocol http jumlah paket data berkurnag menjadi 3469 paket.

Tabel 1. Perbandingan Hasil Jumlah Paket Sebelum Dan Sesudah Di Filter HTTP

Paket	Jumlah Paket	Bukti
Sebelum fillter	1.223.392	Packets: 1223392 · Displayed: 1223392 (100.0%) | Profile: Default
Sesudah filter *http*	3469	Packets: 1223392 · Displayed: 3469 (0.3%) | Profile: Default

Berikut ini proses langkah analisis yang dilakukan

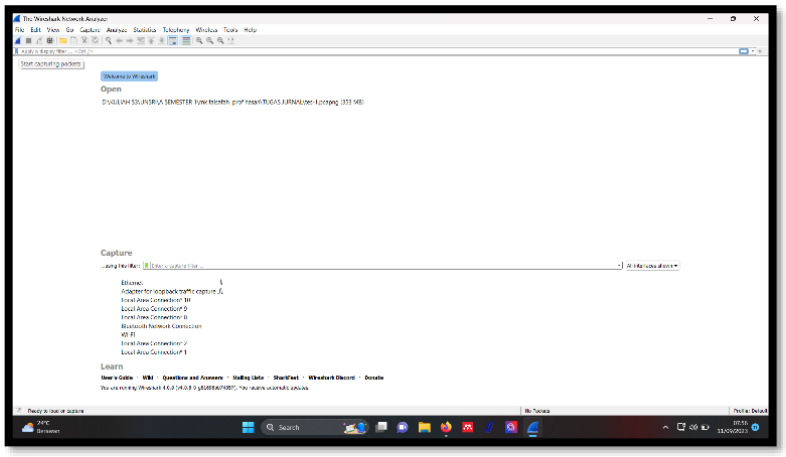
1. Masuk ke jaringan dan Jalankan Aplikasi wireshark
   Universitas Muhammadiyah Palembang telah menggunakan *radius* untuk mengamankan jaringanya terbukti setelah peneliti menghubungkan computer ke *Ethernet* system meminta akun untuk login seperti tergambar pada gambar 1



Gambar 2. Laman Login Radius Untuk Terkoneksi ke Internet UM Palembang

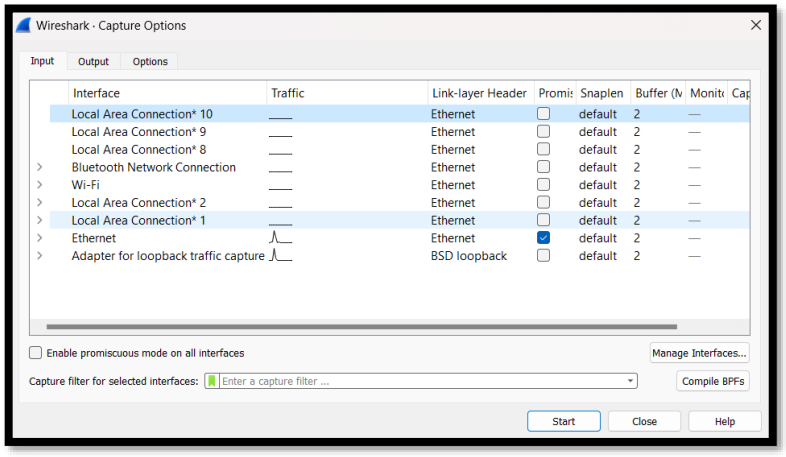
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 10, Oktober 2023
ISSN 2828-2442 (media online)
Hal 2593-2599

Setelah berhasil login jalankna aplikasi *wireshark*



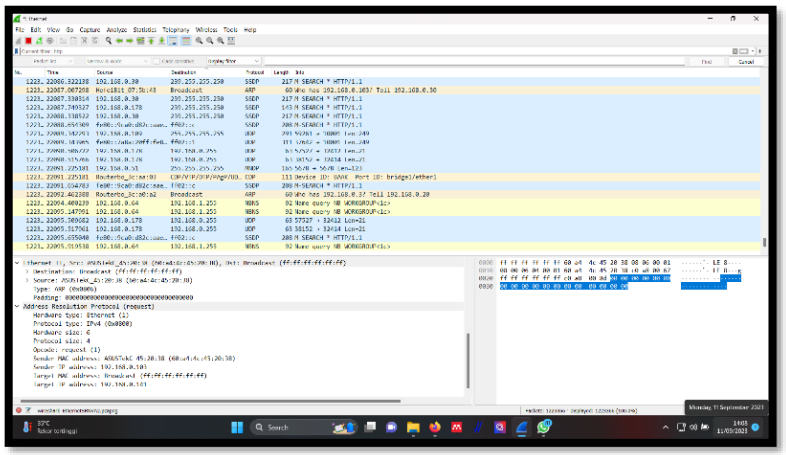
Gambar 3. Menjalankan *Wireshark*

2. Memilih *interface Ethernet (LAN)* dan ceklis serta klik *start* untuk memulai pemantauan paket data internet yang masuk dan keluar komputer



Gambar 4. *Capture Option*

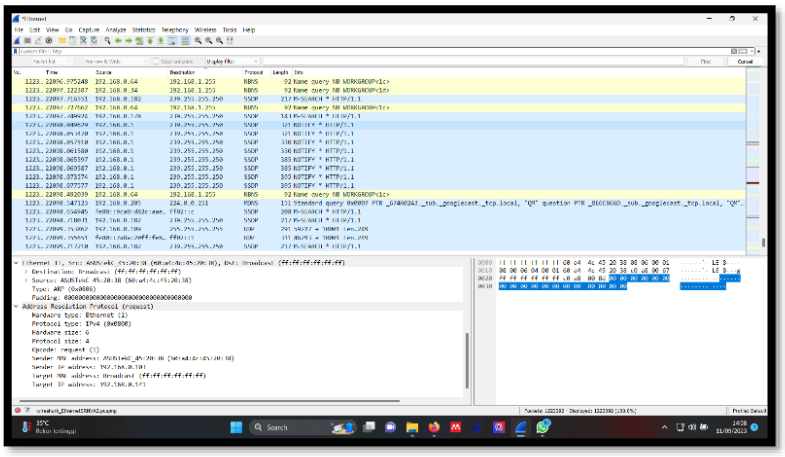
3. Setelah itu wireshark akan melakukan proses capture data, tunggu proses ini dimulai pukul 08.00 wib sampai 14.00 wib



Gambar 5. Awal Pemantauan

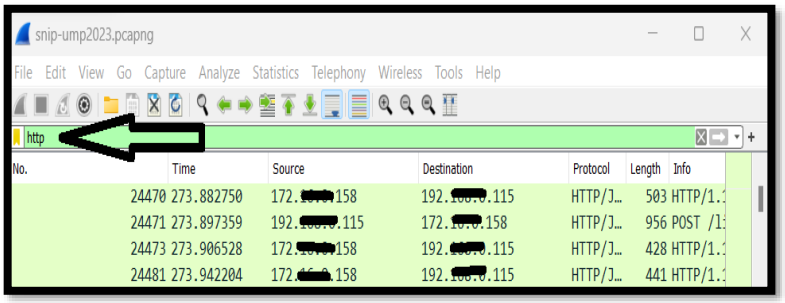
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 10, Oktober 2023
ISSN 2828-2442 (media online)
Hal 2593-2599

4. Setelah pukul 14.00 wib stop proses capture di wireshark



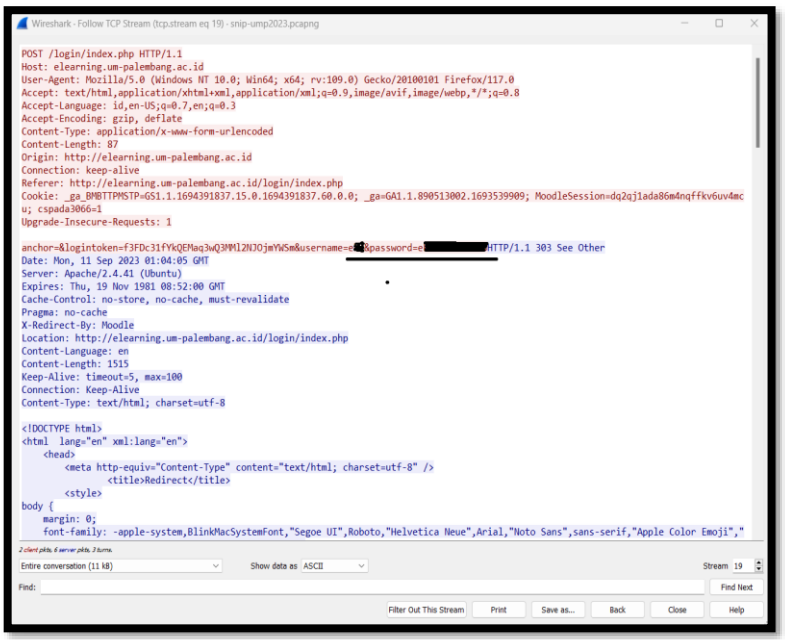
Gambar 6. Akhir Pemantauan

5. Lakukan filtering dengan memasukan http di kolom filtering



Gambar 7. Filtering Data Ke Protokol HTTP

6. Lakukan analisis pencarian data fokus pada *method POST*



Gambar 8. Paket 23966 Berisi Informasi Sensitif

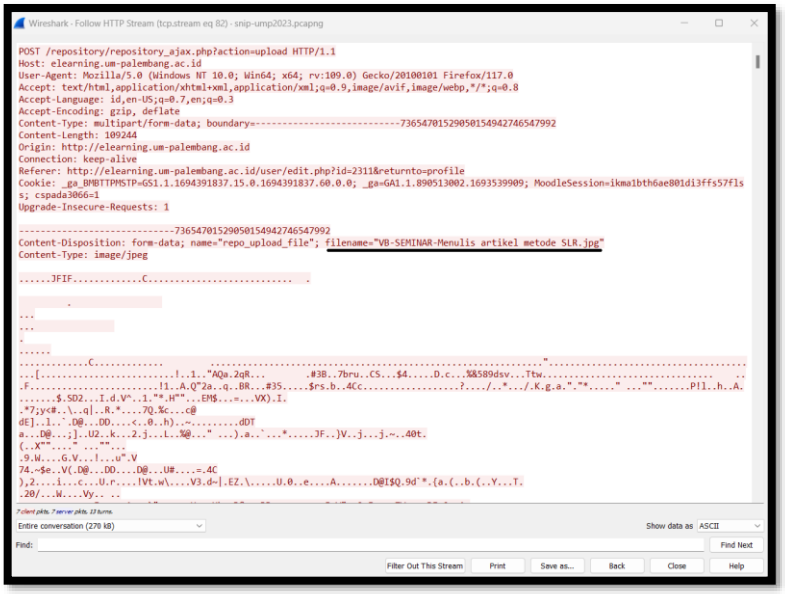
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 10, Oktober 2023
ISSN 2828-2442 (media online)
Hal 2593-2599

7. Setelah dilakukan analisis terhadap paket data peneliti menemukan paket dengan nomor paket 23966 menggunakan method *post* megakses laman /login/index.php paket tersebut berisi informasi *username* dan *password* seperti pada gambar

   Dari gambar diatas, dapat dianalisis serta diambil kesimpulan yaitu sebagai berikut:

   1. *Web browser* yang digunakan oleh *user* ialah *Mozila* dan menggunakan sistem operasi *windows 64bit.*
   2. *Website* yang diakses *http://elearning.um-palembang.ac.id*
   3. Bahasa *website* yang digunakan Indonesia(id) dan inggris(en)
   4. *Full request http://elearning.um-palembang.ac.id/login/index.php*
   5. *Login token* f3FDc31fYkQEMaq3wQ3MMl2NJOjmYWSm
   6. *Username : E*** (tiga karakter) *Password: e*********** (sepuluh karakter)

Selanjutnya paket dengan nomor 28428 terdeteksi pengguna melakukan *edit* data *elearning*, data yang di *edit* ialah perubahan foto profil, detail paket terlihat pada gambar dibawah ini



Gambar 9. Paket 28428 Berisi Informasi Perubahan Data

Berikut penjelasan detail dari gambar diatas

1. Method yang digunakan *post*
2. Website yang diakses *http://elearning.um-palembang.ac.id*
3. Bahasa website yang digunakan Indonesia(id) dan inggris(en)
4. *Fullrequest http://elearning.um-palembang.ac.id/repository/repository_ajax.php?action=upload*
5. Nama file yang diupload *"VB-SEMINAR-MenulisartikelmetodeSLR.jpg"*
6. File data 109244 *bytes*

4. KESIMPULAN

Adapun kesimpulan penelitian monitoring jaringan internet di Kantor Pusat Administrasi Universitas Muhammadiyah Palembang adalah sebagai berikut:

1. Jaringan internet pada Kantor Pusat Administrasi Universitas Muhammadiyah Palembang cukup terjamin keamananya meskipun dapat dilakukan *sniffing* namun jaringan internet telah menggunakan *radius* sehingga pengguna yang tidak memiliki akun tidak akan bisa mengakses internet dan tentunya tidak akan dapat melakukan *sniffing* untuk melakukan *capture* jaringan.
2. Monitoring jaringan internet berhasil dilakukan dengan focus analisis hasil monitoring pada filtrasi berdasarkan protocol *http* .

3. *Wireshark* perangkat lunak yang dapat digunakan untuk melakukan monitoring lalu lintas jaringan internet di Kantor Pusat Administrasi Universitas Muhammadiyah Palembang. Hal ini sejalan dengan temuan peneliti serta penelitian terdahulu yang menggunakan *wireshark* sebagai perangkat lunak untuk memonitoring jaringan.
4. Aplikasi berbasis web yang masih menggunakan protocol *http* di universitas Muhammadiyah Palembang agar segera di *upgrade* ke portokol https agar lebih *secure* mengingat protocol *http* dapat memberikan informasi *sensitive* yang dapat disalahgunakan pihak yang tidak bertanggung jawab .

REFERENCES

Alfian Dharma Kusuma. (2020). *Apa Perbedaan HTTP dan HTTPS? Lengkap Beserta Penjelasannya.* Dicoding.Com. https://www.dicoding.com/blog/perbedaan-http-dan-https/

apjii. (2023). Survei APJII Pengguna Internet di Indonesia Tembus 215 Juta Orang. Apjii. https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang

Bock, L. (n.d.) (2023). *Learn Wireshark: a definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark.* Retrieved August 9, 2023, from https://cdn.ttgtmedia.com/rms/editorial/bookshelf-learnwireshark-excerpt.pdf

Chaudhary, P., Kashyap, V., Sonwal, N., Panwar, P., Dadheech, M., Bhatt, M. M., & Jain, M. M. (2023). This work is licensed under a Creative Commons Attribution 4.0 International License Network Traffic Analysis using Wireshark. *International Advanced Research Journal in Science, 10*(2).

Febriani, Y., & Sahfitri, V. (n.d.). *Seminar Hasil Penelitian Vokasi (SEMHAVOK) MONITORING PENCEGAHAN AKTIVITAS ILEGAL DALAM JARINGAN PADA KANTOR DINAS ESDM PROVINSI SUMATERA SELATAN.*

Huzaeni, F., Gunawan, I., Cahya Purnomo, D., Yanti, M., & Krisdayanti abcde Teknik Elektro Sekolah Tinggi Teknologi Ronggolawe Cepu Penulis Korenspondensi, N. (2021). Analisis Keamanan Data Pada Website Dengan Wireshark. *In Jurnal Elektro Smart) (Vol. 1, Issue 1).* http://sttrcepu.ac.id/siakapt/login

Nurdadyansyah, N., & Hasibuan, M. (n.d.). (2021). *Konferensi Nasional Ilmu Komputer (KONIK).* Perancangan Local Area Network Menggunakan NDLC Untuk Meningkatkan Layanan Sekolah.

Surahman, M., Abdillah, L. A., & Ferdiansyah. (2020). *PENERAPAN METODE SVM-BASED MACHINE LEARNING UNTUK MENGANALISA PENGGUNA DATA TRAFIK INTERNET.* Bina Darma Conference on Computer Science.

Susianto, D., & Rachmawati, A. (2018). *IMPLEMENTASI DAN ANALISIS JARINGAN MENGGUNAKAN WIRESHARK, CAIN AND ABELS, NETWORK MINNER (Studi Kasus: AMIK Dian Cipta Cendikia).* http://www.oxid.it/cain.html