PENGGUNAAN WIRESHARK DALAM PENYADAPAN LALU LINTAS DATA BERPROTOKOL HTTP PADA JARINGAN WI-FI

Syifana Muflih Khaerullah[1], Dinar Mustofa[2]
Universitas Amikom Purwokerto
Jl. Let. Jend Pol. Soemarto Purwokerto
Email: [1]syifanamuflih06@gmail.com, [2]dinar.mustofa@amikompurwokerto.ac.id

Abstract

The internet is an essential necessity in various activities. The ease of exchanging information makes many people choose to use the internet. However, the risk of cybercrime such as sniffing or eavesdropping is a serious threat, especially in Wi-Fi networks. Sniffing aims to retrieve important data over the internet network. This study uses the Wireshark application to conduct sniffing experiments. The research method involves literature study, observation, and implementation of sniffing with Wireshark. The results of the study show that important information such as usernames and passwords that are input to websites that still use the HTTP protocol can be retrieved through sniffing techniques. These findings underscore the importance of using the HTTPS protocol to secure data transmitted over the internet. The practical implications of this study are the increased awareness of internet users and web service providers on the importance of data security and the use of secure protocols to protect sensitive information from sniffing threats. The conclusion of the study was that sniffing with Wireshark successfully uncovered data vulnerabilities in the HTTP protocol.

.

Keywords: *sniffing, Wireshark, internet network, HTTP*

Abstraksi

Internet merupakan kebutuhan penting dalam berbagai aktivitas. Kemudahan dalam bertukar informasi membuat banyak orang memilih menggunakan internet. Namun, risiko kejahatan siber seperti sniffing atau penyadapan menjadi ancaman serius, terutama dalam jaringan Wi-Fi. Sniffing bertujuan mengambil data penting melalui jaringan internet. Penelitian ini menggunakan aplikasi Wireshark untuk melakukan percobaan sniffing. Metode penelitian melibatkan studi literatur, observasi, dan implementasi sniffing dengan Wireshark. Hasil penelitian menunjukkan bahwa informasi penting seperti username dan password yang diinputkan ke website yang masih menggunakan protokol HTTP dapat diambil melalui teknik sniffing. Temuan ini menegaskan pentingnya penggunaan protokol HTTPS untuk mengamankan data yang ditransmisikan melalui internet. Implikasi praktis dari penelitian ini adalah peningkatan kesadaran pengguna internet dan penyedia layanan web terhadap pentingnya keamanan data dan penggunaan protokol yang aman untuk melindungi informasi sensitif dari ancaman sniffing. Kesimpulan penelitian adalah bahwa sniffing dengan Wireshark berhasil mengungkap kerentanan data pada protokol HTTP.

Kata Kunci: *sniffing, Wireshark, jaringan internet, HTTP*

1. PENDAHULUAN

Internet saat ini merupakan kebutuhan yang cukup penting dalam membantu berbagai aktivitas baik dalam konteks Pendidikan, pekerjaan, pemerintahan maupun dalam kehidupan sehari-hari. Aktivitas lain seperti mengakses media sosial, mencari informasi yang diinginkan serta mengakses berita semuanya memanfaatkan jaringan internet [1][2]. Internet banyak dimanfaatkan dalam berbagai perangkat. Kemudahan yang ditawarkan membuat banyak orang lebih memilih internet untuk digunakan dalam bertukar informasi atau mengirim informasi yang penting [3]. Walaupun demikian, dibalik kemudahan ini muncul berbagai permasalahan dan salah satunya adalah praktek *sniffing* atau penyadapan [4].

Sniffing merupakan jenis kejahatan *cyber* yang bertujuan untuk mengambil data atau informasi penting melalui jaringan internet oleh *malware* atau program jahat [5]. *Packet sniffing* merupakan metode pengamatan setiap paket data yang mengalir melalui jaringan dan dapat dilakukan menggunakan perangkat keras atau perangkat lunak yang memantau semua arus lalu lintas dari jaringan [6]. Wireshark merupakan alat yang dapat digunakan dalam menganalisa jaringan yang banyak digunakan oleh *network administrator* dalam menyelesaikan permasalahan yang berada pada sebuah jaringan [7][8]. Dengan menggunakan aplikasi Wireshark,dapat dilakukan pengawasan memeriksa dan menyimpan informasi dari paket yang dikirim maupun diterima pada jaringan [9].

Pentingnya keamanan dalam menggunakan internet tidak bisa dianggap remeh mengingat risiko yang dapat terjadi, salah satunya adalah Tindakan *sniffing*. Tindakan ini dapat memberikan kerugian yang besar, mulai dari pencurian informasi pribadi hingga akses ke akun tertentu. Masalah sniffing telah banyak dibahas dalam literatur terkait keamanan jaringan. Sniffing merupakan ancaman serius dalam jaringan yang tidak terenkripsi, di mana penyerang dapat menangkap dan menganalisis lalu lintas data [10]. Penggunaan alat seperti Wireshark dapat mengidentifikasi kelemahan dalam protokol yang tidak aman, seperti HTTP, dan menekankan perlunya implementasi protokol yang lebih aman seperti HTTPS [11]. Sniffing dapat dengan mudah dilakukan pada jaringan Wi-Fi publik, sehingga menambah urgensi untuk meningkatkan kesadaran dan keamanan pada pengguna jaringan tersebut [12].

Dalam penelitian ini akan dilakukan proses *sniffing* dengan menggunakan *software* Wireshark. Hal ini dilakukan untuk mengetahui cara kerja dari *sniffing* sehingga dapat membantu menyadarkan pentingnya menjaga keamanan informasi saat menggunakan internet terutama dalam jaringan Wi-Fi.

2. METODE PENELITIAN

Metode Penelitian tentang proses *sniffing* menggunakan aplikasi Wireshark untuk mengamati arus lalu lintas yang terjadi pada jaringan internet Wi-Fi meliputi beberapa proses. Proses pengumpulan data dan persiapan bahan serta alat sampai proses mendapatkan hasil. Berikut beberapa metode penelitian yang dilakukan antara lain :

a. Metode Pengumpulan Data

Metode Pengumpulan data dipergunakan dalam mengambil data yang mendukung mengenai permasalahan yang akan diangkat [13]. Berikut adalah metode yang digunakan dalam penelitian:

1) Studi literatur

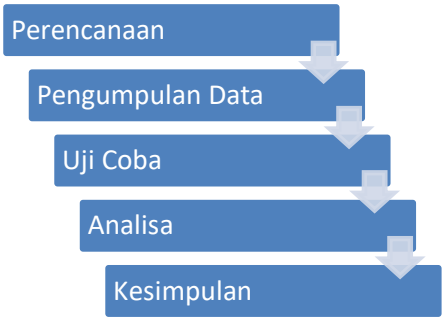
Metode studi literatur melibatkan proses analisa dan pengumpulan literatur terkait *sniffing* pada jaringan internet Wi-Fi. Pengumpulan literatur dilakukan menggunakan pencarian di Google Scholar serta dokumentasi terkait cara *sniffing*.

2) Observasi

Metode observasi merupakan pengambilan data dengan cara terjun ke lapangan secara langsung dan menarik informasi yang tersedia atau melakukan pemantauan langsung pada objek.

b. Alur Penelitian

Alur dari penelitian, diawali dengan melakukan perencanaan, mengumpulkan data terkait *sniffing*, uji coba melakukan *sniffing*, Analisa hasil uji coba dan menyimpulkan hasil dari Analisa. Alur penelitian tersaji pada gambar 1.

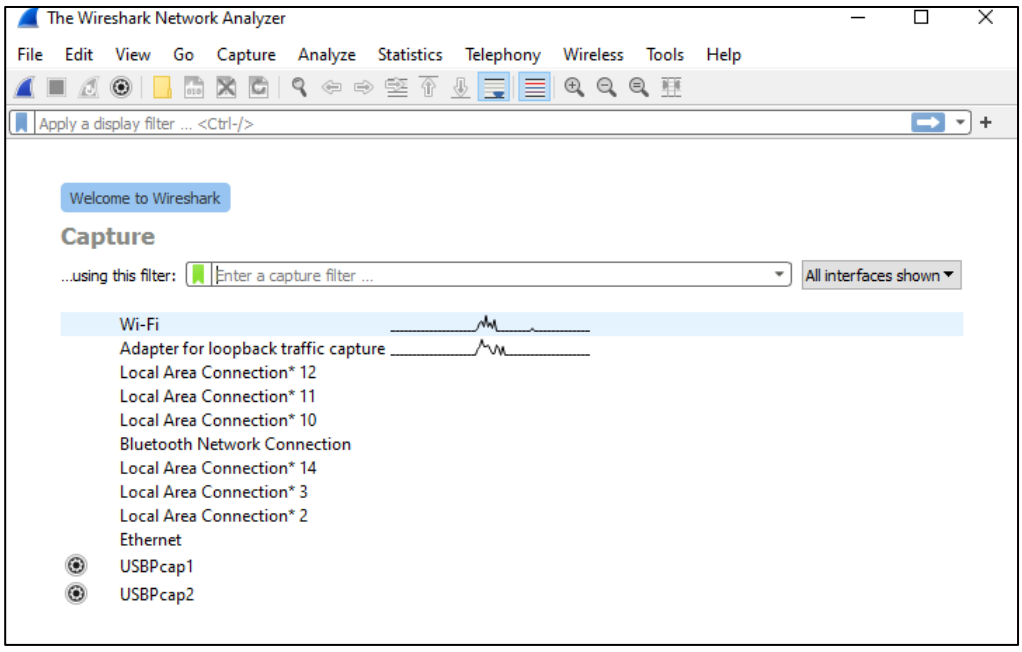


Gambar 1. Alur Penelitian

3. HASIL DAN PEMBAHASAN

Penelitian ini berfokus pada proses sniffing yang digunakan untuk memantau, menerima, dan menampilkan data dalam jaringan internet. Sniffing berisiko tinggi ketika pengguna tidak menyadari bahwa mereka mengirimkan data penting melalui jaringan internet, terutama pada website yang masih menggunakan protokol HTTP dalam komunikasinya. Dalam penelitian ini, akan dilakukan sniffing dengan memanfaatkan software Wireshark untuk mengambil informasi penting seperti nama pengguna dan kata sandi dalam jaringan internet. Berikut adalah langkah-langkah dalam proses sniffing menggunakan Wireshark :

A. Memilih jaringan internet target *sniffing*

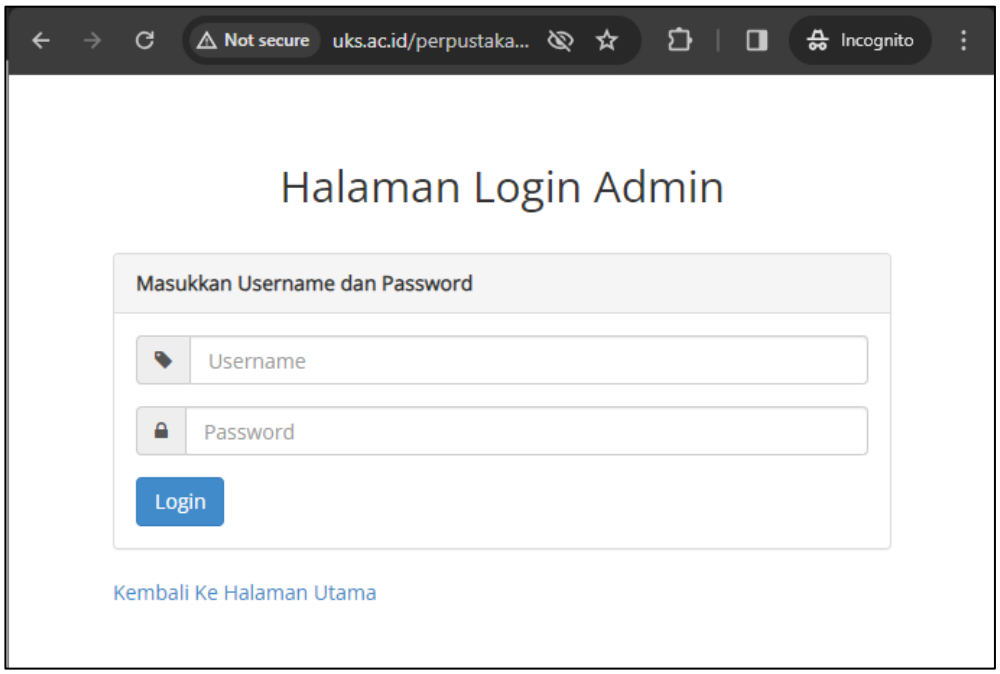


Gambar 2. *interface* pada Wireshark

Pada gambar 2 diatas menunjukkan beberapa interface pada Wireshark, yang merupakan daftar jalur yang tersedia untuk menghubungkan perangkat ke dalam jaringan internet. Garis-garis yang menyerupai elektrokardiogram menandakan aktivitas komunikasi data dalam jaringan internet. Pada penelitian ini, sniffing dilakukan pada jaringan Wi-Fi dengan memilih interface Wi-Fi dan menekan tombol sirip hiu untuk mulai menangkap paket data.

B. Pemilihan Website target

Sebelum memulai *sniffing,* dilakukan pencarian website yang akan dijadikan taget. Kriteria website yang dicari adalah menggunakan protokol HTTP dan terdapat halaman login yang biasanya banyak terdapat pada website lama. Dalam penelitian ini penulis memutuskan untuk mencoba melakukan *sniffing* pada fitur login website perpustakaan milik Univeristas Kristen Teknologi Solo dengan alamat http://uks.ac.id/perpustakaan/login.php. Berikut website target tersaji pada gambar 3.

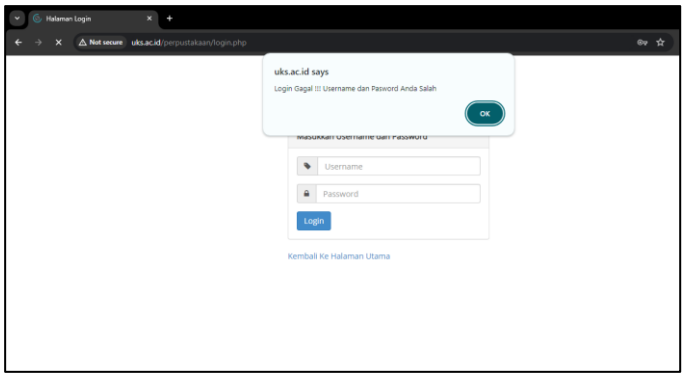


Gambar 3. Website target

Halaman login dari website taget yang masih menggunakan protokol HTTP sehingga terdapat tulisan *Not Secure* disamping alamat dari website sehingga setiap komunikasi data yang terjadi didalam website tidak terenkripsi.

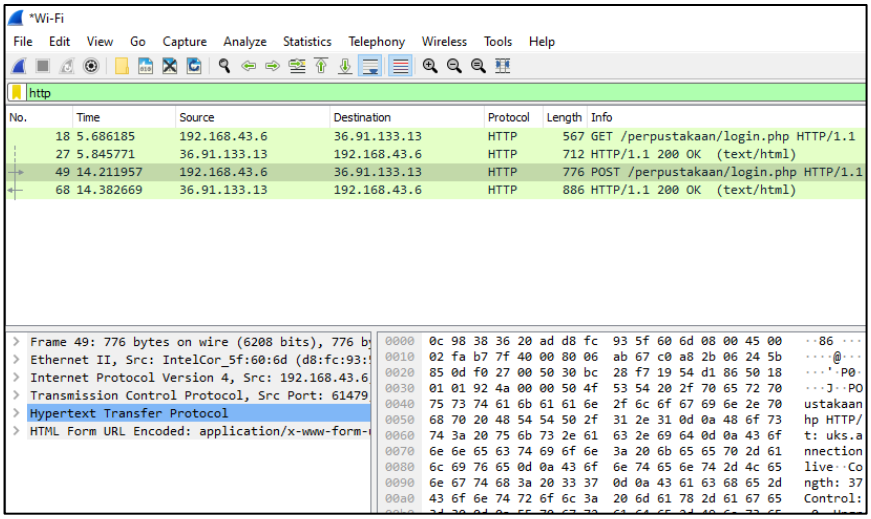
C. Memulai *sniffing*

Setelah menentukan website yang akan dijadikan target, dilakukan percobaan *login* dengan memasukkan kombinasi username dan password secara acak. Sebagai contoh penulis memasukkan kata admin sebagai *username* dan *password*. Hasil login pada website tersaji pada gambar 4.



Gambar 4. Hasil login website

Dari gambar 4 diatas menunjukkan proses login gagal, sesuai harapan karena yang dibutuhkan hanyalah komunikasi data saat login. Saat tombol start capturing packets ditekan, Wireshark secara otomatis merekam komunikasi data yang berlangsung. Selanjutnya, dilakukan pemfilteran untuk menyaring komunikasi data yang menggunakan protokol HTTP sehingga paket ditampilkan di jendela packet list tersaji pada gambar 5.

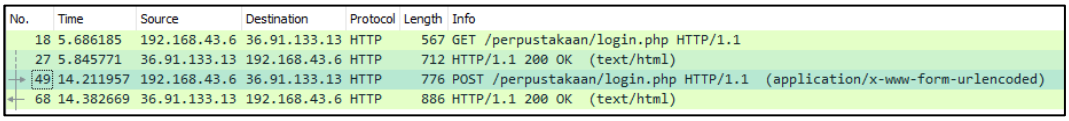


Gambar 5. komunikasi data berprotokol HTTP

Beberapa IP pada *Destination* yang melakukan komunikasi data, dimana 36.91.133.13 merupakan IP dari website target dan terjadi aktivitas GET (mengambil) dan POST (mengirim) data pada kolom *Info*. Di penelitian ini, penulis hanya mencoba komunikasi data pada aktivitas GET saat login.

D. Hasil *Sniffing*

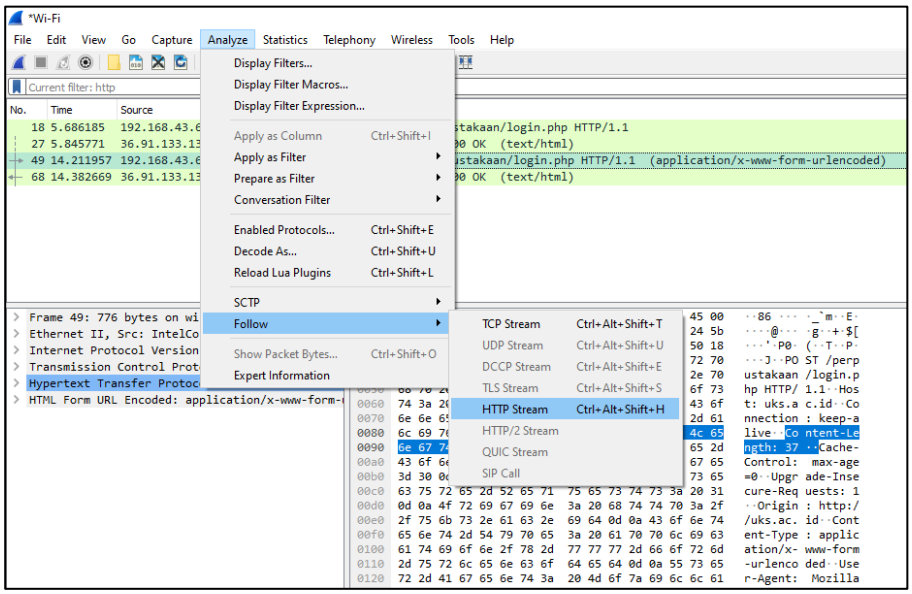
Setelah proses *sniffing*, dilakukanlah analisis pada kolom info terhadap komunkasi data yang telah direkam tersaji pada gambar 6.



No.	Time	Source	Destination	Protocol	Length	Info
18	5.686185	192.168.43.6	36.91.133.13	HTTP	567	GET /perpustakaan/login.php HTTP/1.1
27	5.845771	36.91.133.13	192.168.43.6	HTTP	712	HTTP/1.1 200 OK (text/html)
49	14.211957	192.168.43.6	36.91.133.13	HTTP	776	POST /perpustakaan/login.php HTTP/1.1 (application/x-www-form-urlencoded)
68	14.382669	36.91.133.13	192.168.43.6	HTTP	886	HTTP/1.1 200 OK (text/html)

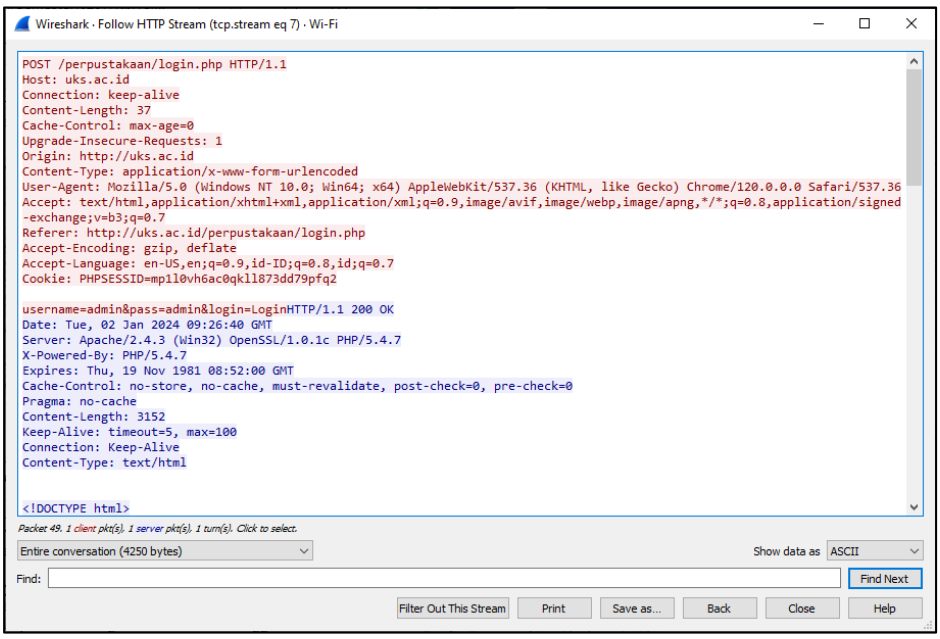
Gambar 6. Kolom info

Analisis berfokus pada paket data berprotokol HTTP dengan aktivitas POST dengan IP tujuan 36.91.133.13 yang terdapat application/x-www-form-urlencoded. Paket data tersebut mengindikasikan jenis dari konten yang dikirimkan sebagai permintaan POST yaitu data formulir yang dikodekan dalam format URL. Analisis HTTP Stream tersaji pada gambar 7.



Gambar 7. Analisis HTTP Stream

Selanjutnya, lakukan Analisa menggunakan HTTP *Stream* pada paket data tersebut. HTTP *Stream* berfungsi untuk melihat secara langsung hal yang terjadi pada protokol PHP saat melakukan aktivitas POST saat *login* tersaji pada gambar 8.



Gambar 8. HTTP Stream

Pada gambar 8 menjukkan hasil dari HTTP *Stream* yang Dimana dibagi menjadi dua blok tulisan dengan warna yang berbeda yaitu merah dan biru. Blok warna merah adalah permintaan (*request*) kepada *webserver*. Sedangkan pada blok biru merupakan respon dari *webserver* ke pengguna. Data pada blok warna merah mengandung informasi seperti fungsi POST ke uks.ac.id, *content-type, user-agent* dan sebagainya. Dari data tersebut dapat diambil informasi seperti jenis browser dan sistem operasi yang digunakan. Selain itu, informasi mengenai *username* dan *password* yang digunakan saat proses login juga ditampilkan. *Username* dan *password* yang digunakan tersaji pada gambar 9.

```
username=admin&pass=admin&login=LoginHTTP/1.1 200 OK
```

Gambar 9. *Username* dan *password* yang digunakan

Dapat dilihat pada gambar diatas, *sniffing* dapat mengambil informasi pengguna saat melakukan *login* dengan jelas dan tanpa adanya enkripsi data. Hal ini membuat *sniffing* pada jaringan Wi-Fi sangat berbahaya terutama pada website yang masih menggunakan protokol HTTP, terlebih proses penyadapan relatif mudah dilakukan namun menghasilkan data yang penting. Penelitian ini menekankan pentingnya penggunaan protokol HTTPS untuk melindungi data yang ditransmisikan melalui jaringan internet. Pengguna internet harus lebih waspada terhadap risiko sniffing dan

selalu memastikan bahwa mereka menggunakan koneksi yang aman. Penyedia layanan web juga harus meningkatkan keamanan dengan mengadopsi protokol yang lebih aman dan mengedukasi pengguna tentang pentingnya enkripsi data.

Secara keseluruhan, penelitian ini berhasil menunjukkan kerentanan protokol HTTP terhadap sniffing dan menyoroti pentingnya praktik keamanan yang baik dalam penggunaan internet. Temuan ini diharapkan dapat meningkatkan kesadaran dan mendorong tindakan proaktif untuk melindungi informasi sensitif dari ancaman sniffing.

4. KESIMPULAN

Berdasarkan hasil penelitian percobaan penyadapan lalu lintas data di jaringan Wi-Fi, menghasilkan kesimpulan sebagai berikut:

A. Penyadapan menggunakan Wireshark pada situs web yang menggunakan protokol HTTP dapat mengungkapkan informasi penting seperti username dan password.
B. Risiko penyadapan dapat diminimalkan dengan meningkatkan keamanan situs web melalui penerapan protokol HTTPS yang mendukung enkripsi data. Selain itu, menghindari koneksi ke jaringan Wi-Fi yang tidak terpercaya juga dapat mengurangi risiko penyadapan.

5. SARAN

Penelitian ini masih terdapat banyak kekurangan, sehingga tidak menutup kemungkinan dilakukannya pengembangan oleh peneliti selanjutnya. Pengembangan dapat berupa penerapan protokol HTTPS dalam mengurangi risiko penyadapan dan eksplorasi metode atau aplikasi penyadapan lain untuk menemukan cara menghindarinya.

DAFTAR PUSTAKA

[1] S. Siddik, M., Lubis, A. P., “OPTIMALISASI KECEPATAN JARINGAN INTERNET PADA MTS,” vol. 4307, no. 1, pp. 117–122, 2023.

[2] F. K. Wardhana, A. Kurniawan, B. R. Seto, and I. A. Saputro, “Analisis Perbandingan Kinerja Enkripsi Algoritma RC4 Dan AES,” *Pros. Semin. Nas. AMIKOM SURAKARTA 2023*, no. November, pp. 124–134, 2023.

[3] I. A. Saputro, I. A. Prabowo, R. A. Aziz, S. A. Surakarta, I. Stmik, and S. Nusantara, “Pengembangan Aplikasi Website Pemetaan Penerima Zakat dengan Metode K- Means Clustering,” vol. 4, no. 2, pp. 1–8, 2024.

[4] Z. M. Luthfansa and U. D. Rosiani, “Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet,” *J. Inf. Eng. Educ. Technol.*, vol. 5, no. 1, pp. 34–39, 2021, doi: 10.26740/jieet.v5n1.p34-39.

[5] M. I. Zulfa, S. Tena, and S. D. Rizkiono, “Aktivitas Sniffing pada Malware Pencuri Uang di Smartphone Android,” *RENATA J. Pengabdi. Masy. Kita Semua*, vol. 1, no. 1, pp. 7–10, 2023, doi: 10.61124/1.renata.4.

[6] A. R. Fauzi and I. made Suartana, “MONITORING JARINGAN WIRELESS TERHADAP SERANGAN PACKET SNIFFING DENGAN MENGGUNAKAN IDS,” *J. Manaj. Inform.*, vol. 8, pp. 11–17, 2018.

[7] R. Hanipah and H. Dhika, “ANALISA PENCEGAHAN AKTIVITAS ILEGAL DIDALAM JARINGAN DENGAN WIRESHARK,” *DoubleClick J. Comput. Inf. Technol.*, vol. 4, no. 1, pp. 11–23, 2020.

[8] A. Zukhruf, B. Fatkhurrozi, A. A. Kurniawan, and U. Tidar, “COMPARATIVE STUDY OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK STUDI KOMPARASI EFEKTIVITAS PENDETEKSIAN SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA JARINGAN KOMPUTER,” vol. 4, no. 5, pp. 1033–1039, 2023.

[9] A. Majid and T. D. Purwanto, “ANALISIS DAN MONITORING SNIFFING PAKET DATA JARINGAN LOKAL BPS SUMSEL DENGAN NETWORK ANALYZER WIRESHARK,” *dalam SEMHAVOK, Palembang*, 2021, [Online]. Available: https://garuda.kemdikbud.go.id/documents/detail/2096324

[10] A. Wijayanto, I. Riadi, and Y. Prayudi, “TAARA Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 7, no. 2, pp. 208–217, Mar. 2023, doi: 10.29207/resti.v7i2.4589.

[11] A. N. Anwar, “Network Security Analysis on The Internet Facility (Wifi) UIN

Syarif Hidayatullah Jakarta Against Packet Sniffing Attacks," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, 2024, [Online]. Available: https://journal.irpi.or.id/index.php/malcom/article/view/1307

[12] N. K. Daulay, R. P. Sari, A. T. Hidayat, and ..., "NETWORK SECURITY DETECTION SYSTEM ON DAPODIK SERVER AT SMPN I MUARA KELINGI AGAINST SNIFFING ATTACKS," *JREEC J. Renew. Energy, Electron. Control*, 2023, [Online]. Available: http://ejurnal.itats.ac.id/jreec/article/view/4552

[13] L. Elfianty, "Sistem Pakar Diagnosa Dampak Penggunaan Eyelash Extension Menggunakan Metode Naive Bayes," *Media Inf. Anal. Dan Sist.*, vol. 8, no. 1, pp. 88–93, 2023.