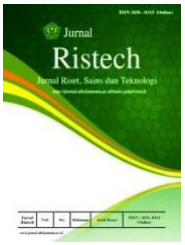
***Jurnal Ristech***
(Jurnal Riset, Sains dan Teknologi)
***Available online at www.jurnal.abulyatama.ac.id/index.php/ristech***
***ISSN 2656 - 0313 (Online)***
***Universitas Abulyatama***




# Analisis Keamanan Jaringan Terhadap Serangan Packet Sniffing Menggunakan Wireshark, Ettercap dan PCAP-Droid

**Ryan Setiawan,[1*], Rahmat Sufri[1], Rahmat Hermanto[1],**
[1)]Program Studi Sistem Informasi, Fakultas Teknik, Universitas Abulyatama, Lampoh Keudee, Aceh Besar, Indonesia
* Email korespondensi: ryan.si@abulyatama.ac.id

Diterima 21 April 2025; Disetujui 14 Juni 2025; Dipublikasi 22 Juli 2025

***Abstract***: *Network security is a primary concern in the management of information systems. One of the common threats in local networks is packet sniffing, a technique used to intercept network traffic using specific software tools. This study aims to analyze the level of network security against packet sniffing attacks using three software tools: Wireshark, Ettercap, and Pcap-Droid. The research method employed is experimental, with testing conducted on both LAN and Wi-Fi networks. The results show that protocols lacking encryption, such as HTTP, are highly vulnerable to interception, while protocols like HTTPS and services protected by SSL/TLS are generally secure. This research highlights the importance of using secure protocols to protect the confidentiality of user data.*

***Keywords: Packet Sniffing; Network Security; Wireshark; Ettercap; Pcap-Droid***

**Abstrak**: Keamanan jaringan menjadi perhatian utama dalam pengelolaan sistem informasi. Salah satu jenis serangan yang rentan terjadi di jaringan lokal adalah packet sniffing, yaitu teknik penyadapan lalu lintas data dalam jaringan menggunakan perangkat lunak tertentu. Penelitian ini bertujuan untuk menganalisis tingkat keamanan jaringan terhadap serangan packet sniffing menggunakan tiga perangkat lunak: Wireshark, Ettercap, dan Pcap-Droid. Metode yang digunakan dalam penelitian ini adalah studi eksperimental, dengan pengujian dilakukan pada jaringan lokal (LAN dan Wi-Fi). Hasil penelitian menunjukkan bahwa protokol yang tidak menggunakan enkripsi seperti HTTP sangat rentan terhadap penyadapan, sementara protokol HTTPS dan layanan yang telah dilindungi oleh SSL/TLS cenderung aman. Penelitian ini memberikan wawasan penting mengenai pentingnya penggunaan protokol aman dalam menjaga kerahasiaan data pengguna.

**Kata Kunci: Packet Sniffing; Keamanan Jaringan; Wireshark; Ettercap; Pcap-Droid**

Dalam era digital, keamanan informasi menjadi hal yang sangat penting, khususnya pada infrastruktur jaringan komputer. Ancaman yang sering terjadi adalah *packet sniffing*, teknik yang digunakan untuk menangkap dan menganalisis paket data yang melintasi jaringan. Aktivitas ini dapat dilakukan oleh pihak yang tidak berwenang untuk mencuri informasi sensitif seperti kredensial pengguna. Penelitian ini memfokuskan pada pengujian keamanan jaringan menggunakan

tiga tools populer: Wireshark, Ettercap, dan Pcap-Droid. Ketiganya digunakan untuk menguji kerentanan jaringan lokal terhadap penyadapan data, baik pada jaringan kabel maupun nirkabel.

Seiring meningkatnya ketergantungan pada layanan digital, keamanan proses autentikasi login pengguna menjadi krusial, terutama dalam sistem seperti manajemen kemahasiswaan kampus. Proses ini melibatkan pertukaran data sensitif, seperti username dan password, yang jika tidak dienkripsi dengan benar dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Meskipun banyak situs web telah menggunakan protokol HTTPS untuk melindungi data, masih ada situs yang menggunakan HTTP, sehingga rentan terhadap penyadapan melalui teknik packet sniffing. Packet sniffing memungkinkan penyerang menangkap dan menganalisis data yang melintas di jaringan, termasuk informasi login. Oleh karena itu, penting dilakukan analisis terhadap trafik jaringan selama proses login untuk mendeteksi potensi kebocoran data. Aplikasi seperti Wireshark, Ettercap, dan Pcapdroid digunakan dalam penelitian ini untuk mengidentifikasi kerentanan komunikasi data. Penelitian ini bertujuan menganalisis keamanan proses login HTTP dan HTTPS terhadap serangan packet sniffing menggunakan ketiga aplikasi tersebut.

Dalam jurnal yang ditulis oleh Moussa & Waazid (2023), keamanan jaringan (network security) merujuk pada kebijakan, prosedur, dan teknologi yang diterapkan untuk melindungi integritas, kerahasiaan, dan ketersediaan data serta sumber daya yang ada dalam jaringan komputer. Keamanan jaringan berfokus pada perlindungan data yang ditransmisikan melalui jaringan dari ancaman seperti penyadapan, perusakan, pencurian data, dan gangguan operasional lainnya. Web server adalah perangkat lunak (software) atau perangkat keras (hardware) yang bertugas untuk menerima permintaan (request) dari klien, seperti browser, dan memberikan respons dalam bentuk halaman web. Web server memainkan peran penting dalam penyediaan layanan informasi di internet. Web server menerima permintaan melalui protokol HTTP/HTTPS dan memberikan konten berupa halaman HTML (Hypertext Markup Language), gambar, video, dan file lainnya kepada pengguna. Menurut Sharma dan Singh (2021), teknik packet sniffing dapat berfungsi untuk memantau trafik jaringan, namun di sisi lain, jika dilakukan oleh pihak yang tidak berwenang, dapat menyebabkan kebocoran data yang sensitif. Sniffing dapat dilakukan pada berbagai protokol jaringan seperti HTTP, FTP, atau protokol lain yang tidak mengenkripsi data secara end-to-end.

Penelitian ini dilakukan karena beberapa alasan. Dari segi akademis, penelitian ini berkontribusi dalam perkembangan ilmu pengetahuan, khususnya di bidang keamanan siber dan jaringan komputer, yang diharapkan dapat memperkaya referensi tentang pentingnya analisis keamanan data, khususnya dalam proses login pada situs web. Dari segi pengembangan situs, penelitian ini berkontribusi dalam

memberikan peringatan tentang pentingnya implementasi protokol keamanan yang tepat, seperti HTTPS, untuk melindungi data pengguna, khususnya selama proses login. Dari segi pengguna, penelitian ini berkontribusi dalam memberikan pemahaman yang lebih baik kepada pengguna internet tentang pentingnya memilih situs web yang aman, khususnya dalam hal autentikasi data.

Adapun pertanyaan penelitian yang diajukan dalam studi ini antara lain: bagaimana proses autentifikasi user pada situs web HTTP dan HTTPS dapat rentan terhadap serangan packet sniffing yang mengakibatkan kebocoran informasi sensitif seperti username dan password? Sejauh mana aplikasi packet sniffer seperti Wireshark, Ettercap, dan Pcapdroid dapat digunakan untuk menganalisis lalu lintas jaringan selama proses autentifikasi user pada situs web HTTP dan HTTPS? Apakah penggunaan protokol enkripsi seperti HTTPS dapat memberikan perlindungan yang efektif terhadap data yang dikirimkan selama proses login, dan bagaimana pengaruhnya terhadap hasil analisis menggunakan alat packet sniffer? Serta, apa saja jenis kerentanannya yang teridentifikasi dalam proses login pada situs web yang tidak menerapkan protokol keamanan yang memadai, berdasarkan analisis data yang ditangkap oleh aplikasi packet sniffer?

## METODE KERJA

### Studi Literatur

Dilakukan pengumpulan data berupa referensi terkait keamanan jaringan, packet sniffer yang relevan dan terbaru baik itu berupa literatur, jurnal dan penelitian terkait.

### Persiapan Alat dan Bahan

Adapun alat penelitian adalah:

- Laptop Asus TUF FX505GT Intel® Core™ i59300H @2.40Ghz Ram 8 Gb
- VM VirtualBox GUI 7.0.20 (Qt5.15.2) Oracle 2024
- Smartphone Samsung Galaxy A05s 6/128 Qualcomm 4x2.4Ghz
- Jaringan Wi-Fi

Adapun bahan penelitian adalah:

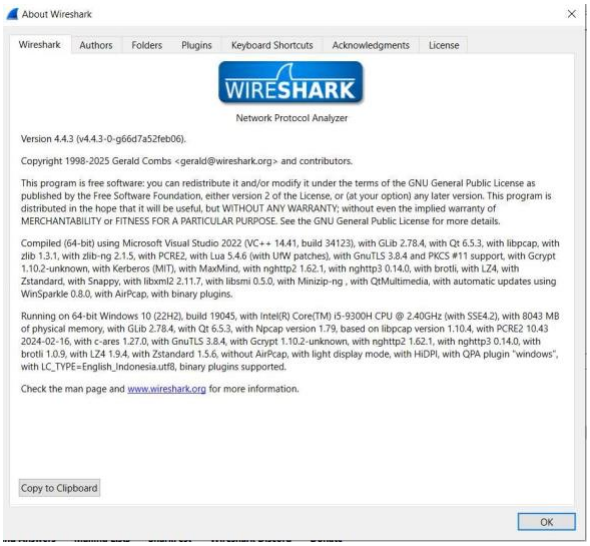
- OS Ubuntu 24.04.1-desktop-amd64
- OS Android 14 UDC
- OS Windows 10.0 Pro 64-bit
- Wireshark 4.4.3 64-bit free software
- Ettercap 0.8.3.1 64-bit
- Pcap Droid 1.7.5 opensource 2024
- Web Browser
  - Chrome official build 64-bit v132.0.6834.83
  - Samsung Web Browser v27.0.0.79
- Link Website
  - http : “http://ekinerja.outsourctrijaya.co.id/”
  - https : “https://vam.telkom.co.id/”

### Konfigurasi

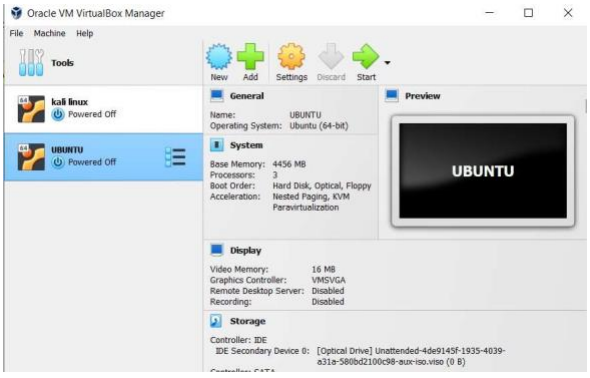
Dilakukan konfigurasi software yang digunakan yaitu instalasi software Wireshark base OS Windows, instalasi VM virtualBox sebagai

media untuk menjalankan OS Ubuntu secara virtual untuk dapat menjalankan aplikasi Ettercap, kemudian melakukan instalasi pcapdroid pada perangkat smartphone yang telah dipersiapkan.

Sistem Operasi yang digunakan dalam penelitian diantaranya, Windows, Ubuntu dan Android. Pada system windows dilakukan instalasi software wireshark dan VM Virtualbox yang dapat dilihat pada gambar dibawah ini.




Gambar 1. Spesifikasi Wireshark



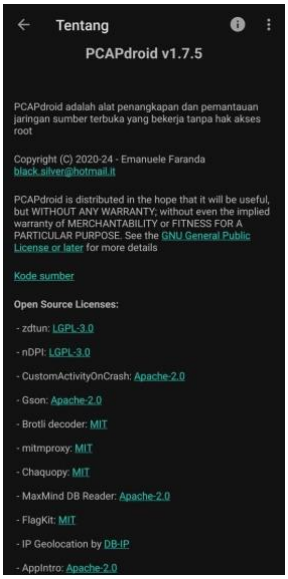

Gambar 2. Tampilan system VM VirtualBox (oracle)

Dari system VM Virtualbox akan dilanjutkan dengan instalasi system operasi ubuntu dan menjalankan aplikasi Ettercap yang ditunjukkan pada gambar berikut.


Gambar 3. Tampilan system operasi Ubuntu (linux)

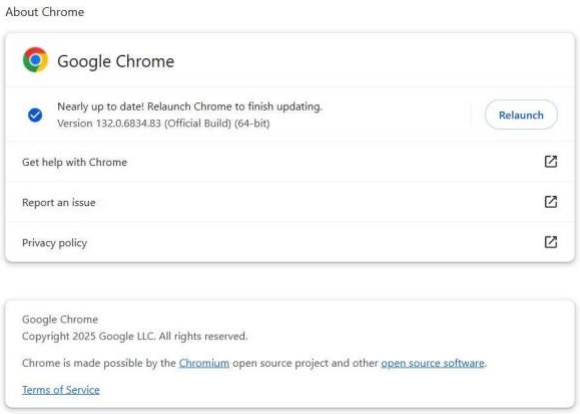

Gambar 4. Tampilan interface Ettercap

Pada aplikasi pcapdroid dapat dilakukan instalasi dari platform googleplay dengan spesifikasi ditunjukkan pada gambar berikut.

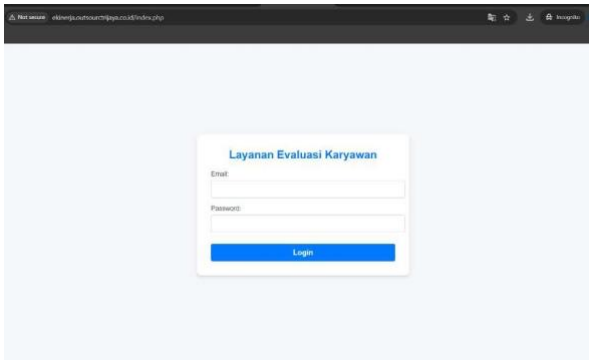



Gambar 5. Spesifikasi aplikasi Pcapdroid (mobile)

Dan dilanjutkan mempersiapkan web browser yang digunakan dan situs dengan protokol http dan https sebagai sarana dalam pengujian system aplikasi sniffing ditunjukkan pada gambar dibawah ini.




Gambar 6. Web browser google chrome




Gambar 7. Situs web http://ekinerja.outsourctrijaya.co.id/dashboard.php


Gambar 8. Situs web https://vam.telkom.co.id/

**Pengujian**

Dilakukan pengujian autentikasi pada web browser yang menggunakan protokol HTTP dan HTTPS bersamaan dengan dijalankannya aplikasi sniffing (wireshark, Ettercap, dan p-capdroid) sehingga dapat menangkap aktifitas jaringan selama proses autentikasi.

**Waktu dan Tempat Penelitian**

Penelitian dilakukan sejak tanggal 17 Juli 2024 dan pengambilan data dilakukan pada dua lokasi berbeda yaitu, Area PT. Outsourc Tri Jaya Jln. Rama Setia, Lr. Bhakti No. 61 Lampaseh Kota, Kec. Kuta Raja Kota Banda Aceh dan Area

NeucentrIX Banda Aceh Jl. Sultan Mahmudsyah No.10, Kp. Baru, Kec. Baiturrahman, Kota Banda Aceh.

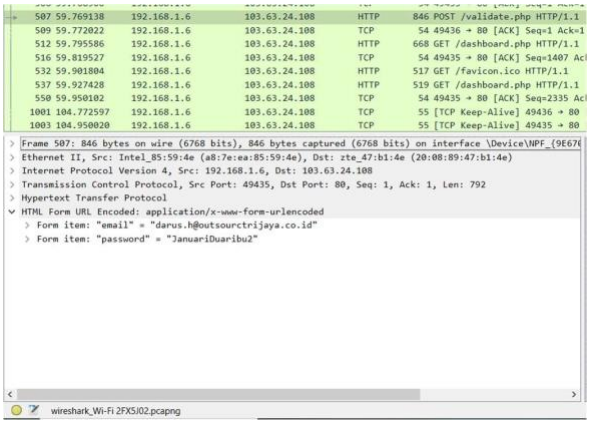
## HASIL DAN PEMBAHASAN

### Alternatif Raw Material

Dari hasil pengujian terdapat 6 hasil capture dengan masing – masing aplikasi mengcapture aktifitas pada web dengan protokol http dan https. Berikut hasil capture dari aplikasi tersebut.

a. Wireshark

Kredensial pada situs web denga protokol http (http://ekinerja.outsourctrijaya.co.id/dashboard.php) dapat dilihat pada gambar berikut.

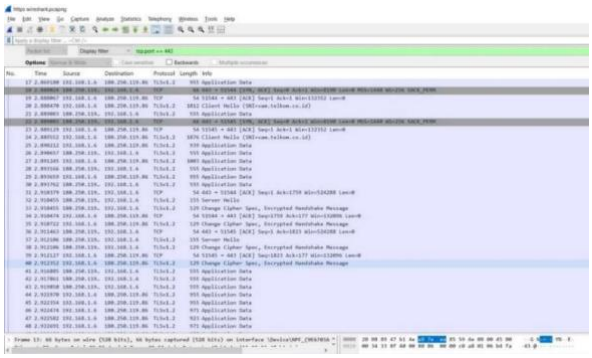



Gambar 9. Hasil capture web http menggunakan wireshark

Kredensial yang ditangkap berdasarkan informasi dari gambar diatas dimulai dari alamat IP sumber 192.168.1.6 (perangkat lain dalam jaringan lokal) dengan alamat IP tujuan 103.63.24.108 (server yang diakses), adapun informasi yang ditampilkan yaitu :

- Email : "darus.h@outsourcitrijaya.co.id"
- Password : "JanuariDuaribu2"

Kredensial pada situs web dengan protokol https (https://vam.telkom.co.id/) dapat dilihat pada gambar berikut.

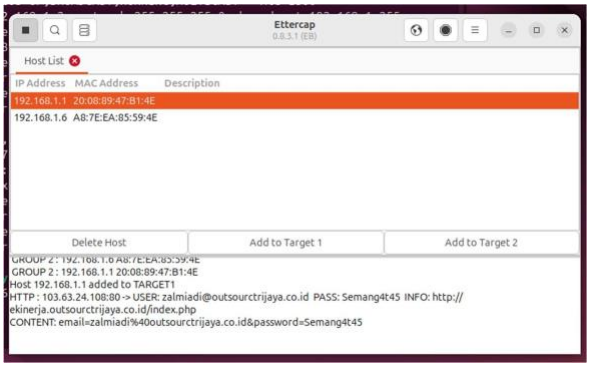


Gambar 10. Hasil capture web http menggunakan wireshark

Tidak terdapat informasi kredensial yang ditangkap dari gambar diatas dikarenakan data login terenkripsi oleh protokol kriptografi SSL/TLSv1.2 dalam proses handshake pada saat authentikasi sehingga aktifitas kredensial pada web https ini menjadi lebih aman dan tidak dapat ditembus oleh wireshark.

b. Ettercap

Pada prinsipnya system Ettercap ini bekerja dengan metode MITM salah satunya dalam bentuk ARP Poison dimana system akan menjembatani lalulintas data dengan alamat ip dan mac address baru. Berikut hasil capture kredensial login pada web http://ekinerja.outsourctrijaya.co.id/dashboard.php.

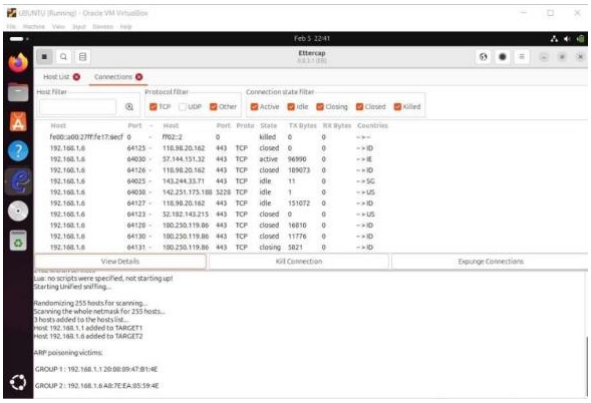



Gambar 11. Hasil capture web http menggunakan Ettercap

Adapun informasi kredensial yang ditangkap sebagai berikut:

- Email yang digunakan: "zalmiadi@outsourctirijaya.co.id"
- Password yang digunakan: "Semang4t45"
- URL login: "http://ekinerja.outsourctirijaya.co.id/index.php"

Pada pengujian web https://vam.telkom.co.id/ dapat dilihat hasil tangkapan datanya pada gambar dibawah ini:

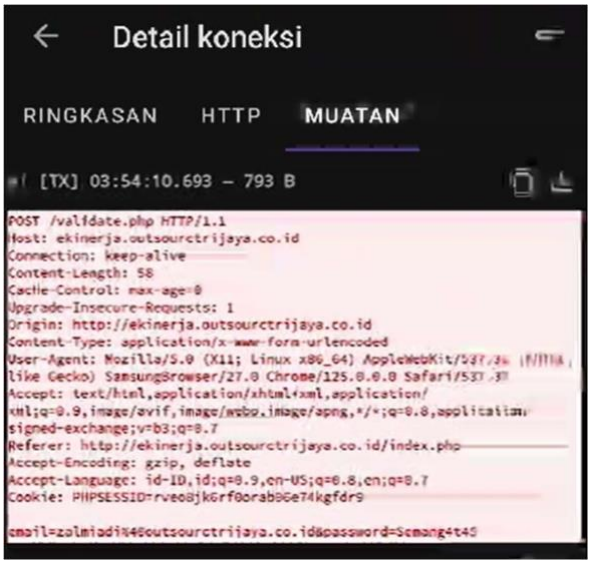


Gambar 12. Hasil capture web https menggunakan Ettercap

Tidak ditemukan kredensial login pada hasil pengujian menggunakan web https dan hanya terekam aktifitas data antar server yang dilalui.

c. Pcapdroid

Berikut hasil capture data web http://ekinerja.outsourctrijaya.co.id/dashboard.php menggunakan aplikasi mobile pcap-droid.




Gambar 13. Hasil capture web http menggunakan Pcapdroid

Dari hasil capture didapatkan informasi kredensial sebagai berikut :

- Email: `zalmiadi@outsourctrijaya.co.id`
- Password: `Semang4t45`
- Cookie: Mengandung `PHPSESSID`, yang bisa digunakan untuk sesi autentikasi.

Adapun hasil capture pcapdroid pada web https://vam.telkom.co.id/ adalah sebagai berikut :

Gambar 14. Hasil capture web https menggunakan Pcapdroid

Dari hasil capture pada gambar diatas tidak

terdapat kredensial login yang terbaca dan hanya mencakup informasi tentang sumber, tujuan, jenis protokol yang digunakan, serta volume data yang dikirim dan diterima.

## KESIMPULAN

Hasil dari tangkapan data berdasarkan lalu lintas jaringan yang digunakan pada aplikasi wireshark, Ettercap dan Pcap Droid dapat diambil kesimpulan bahwa data kredensial pengguna telah terekspos dalam bentuk teks biasa saat dikirim melalui protokol HTTP. Hal ini menunjukkan bahwa situs yang diakses pada web HTTP ini sangat rentan terhadap penyadapan data melalui serangan Man-in-the-Middle (MitM).

Informasi seperti email, password, dan session ID (PHPsessID) juga dapat dengan mudah diambil oleh user yang memiliki akses ke lalu lintas jaringan tersebut. Sedangkan pada web yang menggunakan protokol HTTPS data terenkripsi dan tidak dapat di ekspos oleh ketiga aplikasi sniffing tersebut sehingga proses autentikasi login user jauh lebih aman dibandingkan dengan web yang menggunakan protokol HTTP.

Resiko keamanan yang ditemukan dari autentikasi user pada web http diantaranya data login tidak terenkripsi, membuatnya rentan terhadap aktifitas sniffing, sehingga menyebabkan komunikasi antara pengguna dan server dapat disadap, dan tampilan Session ID yang terekspos, sehingga dapat digunakan untuk membajak sesi pengguna tanpa perlu memasukkan kata sandi.

## DAFTAR PUSTAKA

[1] Moussa, A., & Wazid, M. (2023). "A Survey on Security Threats and Solutions in Cloud Computing and Internet of Things". International Journal of Computer Applications, 175(1), 56-63

[2] Kurose, J. F., & Ross, K. W. (2017). "Computer Networking: A Top-Down Approach". Pearson.

[3] Sharma, R., & Singh, M. (2021). "Packet Sniffing and Network Security: Techniques and Tools". Journal of Cyber Security Technology, 5(3), 123-135.

[4] Bargig, A., Shaar, M., & Zaher, H. (2022). "Utilizing Ettercap in Network Traffic Sniffing and Man-in-the- Middle Attacks". International Journal of Information Technology and Security, 15(2)

[5] Sundaram, K., Rajendran, S., & Kumar, N. (2023). "Pcapdroid: Mobile Packet Sniffing and Security Analysis". Journal of Wireless Communication and Mobile Computing, 2023

[6] Husain, M., Sharma, S., & Kapoor, V. (2021). "The Importance of Securing Web Login Systems: A Review of Authentication Methods and Encryption Protocols". Journal of Information Security, 12(4), 65-78

[7] Thomas, A., & Singh, R. (2021).“Securing Online Transactions with HTTPS: Analyzing the Role of Digital Certificates in Web Security”. Cybersecurity Review, 5(3), 65-80

[8] Kurose, J. F., & Ross, K. W. (2017). “Computer Networking: A Top-Down Approach”. Pearson.

[9] Shinder, D. L., & Cross, M. (2008). “Microsoft Internet Information Services (IIS) 7.0 Administrator's Pocket Consultant”. Microsoft Press.

[10] Chen, X., & Zheng, Y. (2023). “An Overview of Web Security Protocols: HTTP, HTTPS, and Their Role in Securing Web Applications”. Journal of Cybersecurity and Privacy, 1(4), 112-127