Analisis Perbandingan Keamanan Data pada *Website Repository* UNHI dan *Website SRUTI* UNHI Terhadap *Sniffing Process* Menggunakan Aplikasi *Wireshark*

I Made Ramanda Bayu Suputra[a1], I Kadek Andy Asmarajaya [a2], I Kadek Noppi Adi Jaya [a3]
[a]Program Studi Sistem Informasi, Fakultas Teknologi Informasi dan Sains,
Universitas Hindu Indonesia, Indonesia
e-mail: [1]ramandabayu04@gmail.com, [2]andyasmarajaya@unhi.ac.id, [3]iknadijaya@unhi.ac.id

Abstrak

Perkembangan teknologi informasi yang pesat meningkatkan risiko keamanan data dalam jaringan komputer, terutama melalui penyadapan informasi (sniffing). Universitas Hindu Indonesia (UNHI) memiliki dua platform web, Repository UNHI dan SRUTI UNHI, yang menggunakan protokol berbeda (HTTP dan HTTPS). Penelitian ini menganalisis dan membandingkan keamanan data pada kedua website terhadap serangan sniffing menggunakan aplikasi Wireshark, serta memberikan wawasan tentang kerentanan protokol HTTP dan keunggulan protokol HTTPS. Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif yang diterapkan melalui Network Development Life Cycle (NDLC). Wireshark digunakan untuk menangkap dan menganalisis paket data pada jaringan kedua website. Hasil analisis menunjukkan bahwa website Repository UNHI yang menggunakan HTTP sangat rentan terhadap serangan sniffing, dengan Wireshark berhasil menangkap dan membaca data sensitif seperti username dan password. Sebaliknya, website SRUTI UNHI yang menggunakan HTTPS menunjukkan tingkat keamanan lebih tinggi karena data yang dikirim telah dienkripsi. Penelitian ini menunjukkan bahwa penggunaan protokol HTTPS secara signifikan meningkatkan keamanan data dibandingkan dengan HTTP.

Kata kunci: *Keamanan Data, Repository UNHI, SRUTI UNHI, Sniffing Process, Wireshark*

Abstract

The rapid development of information technology has increased the risk of data security in computer networks, especially through information sniffing. Universitas Hindu Indonesia (UNHI) has two web platforms, Repository UNHI and SRUTI UNHI, which use different protocols (HTTP and HTTPS). This research analyzes and compares data security on both websites against sniffing attacks using the Wireshark application and provides insights into the vulnerabilities of the HTTP protocol and the advantages of the HTTPS protocol. This research uses a descriptive method with a qualitative approach applied through the Network Development Life Cycle (NDLC). Wireshark is used to capture and analyze data packets on the network of both websites. The analysis results show that the Repository UNHI website, which uses HTTP, is highly vulnerable to sniffing attacks, with Wireshark successfully Capturing and reading sensitive data such as usernames and passwords. Conversely, the SRUTI UNHI website, which uses HTTPS, demonstrates a higher level of security as the data transmitted is encrypted. This research indicates that the use of the HTTPS protocol significantly enhances data security compared to HTTP.

Keywords : *Data Security, UNHI Repository, SRUTI UNHI, Sniffing Process, Wireshark*

1. Pendahuluan

Pesatnya perkembangan teknologi informasi saat ini telah mengakibatkan transformasi signifikan di banyak sektor, termasuk dalam bidang keamanan data informasi. Pada saat yang sama, protokol *internet* seperti *HTTP* dan *HTTPS* digunakan secara luas untuk mengakses situs

web dan platform berbasis *web*. Meskipun memberikan kenyamanan, penggunaan protokol ini meningkatkan risiko pengiriman data yang tidak aman, rentan terhadap pengambilan data oleh pihak yang tidak bertanggung jawab, terutama dalam hal penyadapan informasi (*sniffing*) di jaringan komputer [1]. Penyadapan informasi ini menjadi semakin mengkhawatirkan karena dapat mencakup data pribadi. Informasi yang sering diambil meliputi nama pengguna (*username*) dan kata sandi (*password*) dari akun korban, yang kemudian digunakan untuk tujuan yang merugikan. [2]. Pencurian data tersebut dapat merugikan berbagai sektor, termasuk salah satunya yaitu sektor pendidikan.

Universitas Hindu Indonesia (UNHI) merupakan lembaga pendidikan tinggi swasta yang berada di Denpasar Timur, Bali. Pendirian universitas ini dilakukan pada tahun 1963, UNHI memiliki tujuh fakultas dan menonjol dengan integrasi nilai budaya lokal dalam pendidikannya. UNHI juga menonjol dengan konsep "keBALIan," yang mencerminkan semangat inovasi dan transformasi sambil mempertahankan akar budaya dan nilai-nilai tradisional Bali [3]. Salah satu aspek transformasi yang signifikan adalah dalam hal penggunaan teknologi digital dalam manajemen dan proses akademik. UNHI beralih dari metode tradisional ke teknologi *digital* untuk meningkatkan efisiensi pendidikan, dengan mengadopsi sistem informasi terintegrasi bernama *SRUTI* UNHI. *SRUTI* UNHI menjadi keputusan strategis dalam merespon digitalisasi dalam dunia pendidikan dengan memfasilitasi manajemen data, administrasi akademik, dan interaksi mahasiswa secara efisien [4].

SRUTI UNHI mengadopsi *HTTPS* untuk melindungi data pengguna. Langkah ini dilakukan untuk melindungi data pengguna dari potensi risiko keamanan. Namun dalam konteks keamanan data, masih ada beberapa *website* milik Universitas Hindu Indonesia yang masih menggunakan protokol *HTTP*, salah satunya yaitu *Repository* UNHI. *Repository* UNHI Denpasar menjadi layanan yang menyediakan berbagai penyimpanan berkas, antara lain makalah, skripsi, tesis, buku, prosiding, konferensi, hasil karya ilmiah di bidang akademik, dan berbagai dokumen lainnya. Namun *website Repository* UNHI saat ini masih menggunakan protokol *HTTP*, tidak terjamin bahwa data yang dikirim antara klien dan *server* terlindungi dengan aman. Hal ini mengakibatkan berbagai masalah kriminal, termasuk kebocoran data pribadi yang dimasukkan ke dalam situs *web* melalui protokol *HTTP*. [5].

Pentingnya keamanan data dalam lingkup *Repository* UNHI dan *SRUTI* UNHI terkait dengan risiko pencurian data pribadi, seperti *username* dan *password*, dapat merugikan pengguna di dunia maya, maka dari itu diperlukan analisis keamanan data. Analisis keamanan data, menggunakan alat seperti *Wireshark*, penting untuk mendeteksi kerentanan dan mencegah pencurian data pribadi [6]. *Wireshark* dapat menangkap paket data di jaringan, memungkinkan deteksi potensi pencurian identitas dan data penting [7]. Untuk menghadapi tantangan keamanan data pada platform digital seperti *website Repository* UNHI dan *website SRUTI* UNHI, penting untuk mengimplementasikan pendekatan yang sistematis dalam pengembangan dan pengelolaan jaringan, salah satunya adalah *Network Development Life Cycle* (*NDLC*). Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif yang diterapkan melalui *Network Development Life Cycle* (*NDLC*), sebuah pendekatan penelitian yang bertujuan memberikan gambaran rinci dan menyeluruh tentang fenomena atau kejadian tertentu [8].

Penelitian ini bertujuan untuk memberikan analisis perbandingan tentang proses dilakukannya penyadapan terhadap data *username* dan *password* pada *website Repository* UNHI dan *website SRUTI* UNHI dengan menggunakan aplikasi Wireshark, sehingga pengguna (*user*) dapat lebih berhati-hati untuk membagikan informasi yang bersifat pribadi dan penting.

2. Metodologi Penelitian

2.1 Metode Pengumpulan Data

Teknik pengumpulan data menggunakan metode data *primer* dan *sekunder*.

A. Data *Primer*

Data *primer* adalah informasi yang didapat langsung dari sumber aslinya untuk keperluan penelitian spesifik. Perolehan data melalui observasi, wawancara, survei, atau eksperimen yang dilakukan langsung oleh peneliti [9]. Dalam penelitian ini, data *primer* didapat melalui metode wawancara dan observasi.

1. Wawancara

   Metode wawancara merujuk pada proses pengumpulan data dengan cara interaksi langsung bersama responden.

2. Observasi
Proses ini dimulai dengan mencatat, menganalisa, dan membuat kesimpulan mengenai pelaksanaan serta hasil program, bergantung pada apakah program tersebut berkembang atau tidak.

B. Data *Sekunder*

Data *sekunder* adalah informasi yang didapatkan oleh pihak lain atau untuk tujuan yang berbeda sebelumnya, yang kemudian digunakan kembali dalam penelitian baru. [10]. Dalam penelitian ini, data *sekunder* didapat melalui metode dokumentasi serta studi kepustakaan.

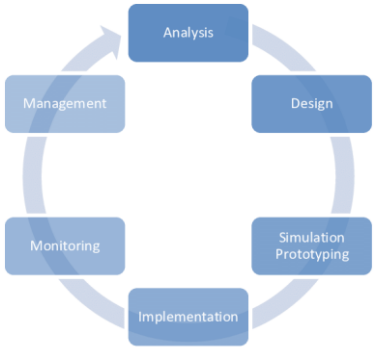
1. Dokumentasi
Dokumentasi melibatkan pengumpulan data dari dokumen-dokumen penting yang berasal dari institusi, organisasi, dan individu. Dokumen dalam penelitian ini berupa foto yang diambil untuk memperjelas temuan penelitian.
2. Studi Kepustakaan
Studi kepustakaan adalah proses analisis dan sintesis informasi yang didapatkan dari beragam sumber literatur, seperti, artikel, jurnal, buku, serta dokumen sejenis, yang berhubungan dengan topik penelitian tertentu.

2.2 Prosedur Penelitian

Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif yang diterapkan melalui *Network Development Life Cycle* (*NDLC*). Metode deskriptif bertujuan untuk mendetailkan karakteristik keamanan data pada kedua *website*, mencakup kebijakan keamanan, enkripsi, manajemen akses, dan langkah-langkah keamanan lainnya. Pendekatan kualitatif memungkinkan pemahaman mendalam tentang konteks dan pengalaman terkait keamanan data di *website Repository* UNHI dan *SRUTI* UNHI melalui observasi, wawancara, studi kepustakaan, dan analisis dokumen.

NDLC menyediakan struktur konseptual yang fleksibel untuk desain jaringan dengan enam tahapan: analisis, desain, simulasi prototipe, implementasi, *monitoring*, serta manajemen [11]. Metode ini membantu dalam pembangunan sistem jaringan komputer dengan mempertimbangkan kebutuhan spesifik setiap jaringan [12].

Alur penelitian dimulai dengan identifikasi permasalahan, penetapan tujuan dan ruang lingkup, serta pengumpulan data *primer* dan data *sekunder*. Pengembangan sistem ini mengikuti lima tahapan *NDLC*: analisis, desain, simulasi, implementasi, dan *monitoring*. Gambar 1 menunjukkan ilustrasi metode *NDLC*.



Gambar 1 Ilustrasi Metode *NDLC*

Penjelasan mengenai Gambar 1 :

1. Analisis
Tahap analisis terdiri dari beberapa fase, yaitu: *Identify* (mengidentifikasi masalah), *Understand* (memahami masalah), *Analyze* (menganalisis kebutuhan sistem), dan *Report* (melaporkan hasil analisis).

a. *Identify*
Identifikasi permasalahan berawal dari *website* Repository UNHI menggunakan protokol *HTTP*, tidak aman bagi keamanan data, berbeda dengan *SRUTI* UNHI yang sudah mengadopsi *HTTPS*.

b. *Understand*
Dengan menggunakan teknik pengumpulan data yang melibatkan 2 (dua) jenis data, yaitu

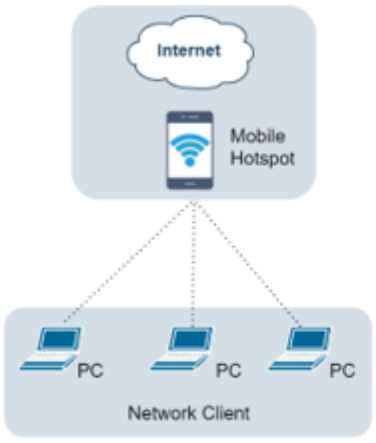
data *primer* dan data *sekunder*. Informasi ini digunakan untuk memahami permasalahan dan merumuskan solusi yang efektif.

c. *Analyze*
Pemahaman yang diperoleh digunakan sebagai dasar untuk menganalisis solusi sistem yang dapat menyelesaikan rumusan masalah. Berikut adalah hasil analisisnya:
1. Penelitian ini bertujuan untuk melakukan pengujian terhadap keamanan data sistem dengan memanfaatkan aplikasi *Wireshark*, dengan fokus utama penelitian ini adalah pada keamanan data yang terdapat pada dua website, yaitu *Repository* UNHI dan *SRUTI* UNHI.
2. Pengujian ini akan difokuskan pada pengecekan keamanan data yang berkaitan dengan *username* dan *password* pengguna. Pengujian dilakukan dengan menggunakan jaringan hotspot pada perangkat *mobile* dengan koneksi ke *network client* jaringan dilakukan secara nirkabel.

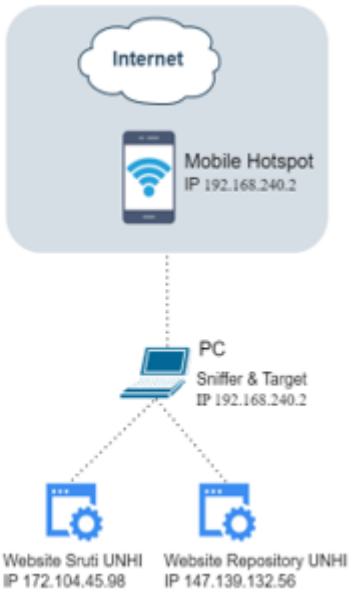
d. *Report*
Fase akhir dari analisis adalah penyusunan laporan yang mencakup detail dari komponen yang diperlukan. Komponen yang digunakan dalam penelitian ini dapat dibagi menjadi 2 (dua) jenis, yaitu perangkat lunak (*software*) serta perangkat keras (*hardware*).
1. Kebutuhan perangkat keras dan sistem operasi :
   a. *Laptop Lenovo IdeaPad* S145-14API
   b. *Processor AMD Ryzen* 5 3500U
   c. GPU Radeon Vega Mobile Gfx 2.10 *GHz*
   d. *RAM* 8 *GB*.
   e. HDD 1 *TB.*
   f. Sistem operasi *Windows* 11 64-bit.
   g. *Smartphone Samsung Galaxy* A52s
2. Kebutuhan perangkat lunak :
   a. *Software Wireshark* versi *4.2.4*
   b. *Browser Chrome*

2. Desain

Perancangan sistem ini akan dilakukan dalam konteks virtualisasi. Pada tahap perancangan ini, terdapat dua proses utama, yaitu perancangan fisik dan perancangan logis.



Gambar 2 Ilustrasi Perancangan Fisik



Gambar 3 Ilustrasi Perancangan Logis

Rincian keterangan dari perancangan fisik topologi jaringan yang digunakan pada Gambar 2, yaitu :

a. Topologi yang digunakan adalah *Star*.
b. Koneksi yang digunakan dari *mobile hotspot* menuju *network client* adalah melalui media transmisi nirkabel (*wireless*).

Pada Gambar 3, desain logis perancangan jaringan yang digunakan terlibat perangkat yang saling terhubung, yaitu: jaringan *internet*, *mobile hotpsot* yang berasal dari ponsel pintar (*smartphone*), dan satu laptop yang berfungsi sebagai penyerang dan target (*target-initiator*) [13].
3, Simulasi
Pada tahap ini proses simulasi jaringan dilakukan dan diterapkan menggunakan aplikasi *Wireshark*. Aplikasi *Wireshark* versi 4.2.3 digunakan dalam proses simulasi untuk menangkap jaringan yang akan diretas sebagai prototipe simulasi.
4. Implementasi
Fokus utama dari tahapan ini adalah instalasi aplikasi *Wireshark*, yang merupakan alat utama yang digunakan untuk melakukan analisis lalu lintas jaringan, serta prosedur akses kedua *website* utama yang menjadi objek penelitian, yaitu *website SRUTI* UNHI dan *website Repository* UNHI. Implementasi ini mencakup beberapa langkah untuk melakukan penyadapan (*sniffing*) dan analisis data yang mengalir melalui jaringan.
5. *Monitoring*
Tahap monitoring melibatkan beberapa proses, seperti melakukan penyerangan (*sniffing*) terhadap *website SRUTI* UNHI dan *website Repository* UNHI, serta mengamati dan menganalisis menggunakan aplikasi *Wireshark*. Pengujian dilakukan menggunakan jaringan *internet mobile hotspot*.

3. Kajian Pustaka

3.1 *Sniffing Process*

Sniffing merupakan proses memantau dan menangkap semua paket yang melalui jaringan tertentu menggunakan alat *sniffing*. [14]. *Sniffing* memungkinkan pengguna untuk melihat semua jenis lalu lintas, baik yang terproteksi maupun yang tidak. Dalam keadaan serta protokol yang sesuai, pelaku serangan bisa mengumpulkan data dan informasi yang dapat difungsikan untuk serangan lebih lanjut maupun mengakibatkan masalah terhadap pemilik jaringan maupun sistem.

3.2 *HTTP*

Hypertext Transfer Protocol (*HTTP*) merupakan protokol dalam jaringan aplikasi yang berfungsi untuk menyalurkan informasi antara komputer *server* dan *client*. Di sini, *server* adalah *web server* yang merupakan bagian dari jaringan komputer berskala besar. Sementara *client* merupakan *web browser* yang bisa mengakses, mendapatkan, dan memperlihatkan konten melalui *browser* [5].

3.3 *HTTPS*

Hypertext Transfer Protocol Secure (*HTTPS*) adalah versi *HTTP* yang lebih aman. Dengan *HTTPS*, tingkat keamanan yang disediakan jauh lebih tinggi jika dibandingkan dengan *HTTP*. sehingga memberikan rasa aman lebih kepada *client* saat mengakses konten *web*. *HTTPS* menggunakan protokol keamanan untuk melindungi data yang ditransmisikan, menjadikannya pilihan yang lebih populer di kalangan *web developer*. [5].

3.4 *Repository* UNHI

Repository adalah layanan penyimpanan berkas *digital* yang dapat diunduh untuk digunakan atau dapat diartikan sebagai sebuah arsip *file* yang ada pada media *website* [15]. *Repository* UNHI bisa dikatakan struktur data yang menyimpan metadata untuk sekelompok struktur berkas atau direktori yang dimiliki civitas akademika Universitas Hindu Indonesia.

3.5 *SRUTI* UNHI

SRUTI UNHI adalah singkatan dari Sistem Informasi Universitas Terintegrasi yang memberikan kekuatan integrasi, kemudahan, dan fleksibilitas milik Universitas Hindu Indonesia. *SRUTI* bertekad untuk membangun dan memperkuat sistem pengelolaan universitas serta mendorong penerapan akuntabilitas dan transparansi dalam manajemen universitas. *SRUTI* berfokus pada penguatan fondasi perguruan tinggi untuk menciptakan pelayanan yang optimal, bermartabat, *modern*, dan profesional.

3.6 *Wireshark* Versi 4.2.4

Wireshark adalah aplikasi yang digunakan sebagai alat untuk menganalisis paket jaringan yang sedang berjalan. Versi aplikasi *Wireshark* yang terbaru adalah versi 4.2.4. *Wireshark* juga dikenal sebagai penganalisa paket jaringan, fungsinya untuk menampilkan hasil informasi secara lengkap dan menangkap (*capture*) paket yang diterima atau dikirim. Dengan *Wireshark*, memudahkan administrator dalam memantau jaringan, karena data yang dikumpulkan dapat dibuka dan disimpan kembali untuk dianalisia [16].

4. Hasil dan Pembahasan

4.1 Instalasi *Wireshark*

Tahapan instalasi melibatkan penerapan rencana topologi dan sistem yang telah dirancang dalam lingkungan nyata menggunakan simulasi *mobile hotspot*. Implementasi mencakup instalasi dan konfigurasi aplikasi *Wireshark* sesuai spesifikasi. *Wireshark* dapat diunduh dengan cara men-download dengan gratis melalui situs resmi *web Wireshark* pada alamat *https*://www.*wireshark*.*org*. Versi yang digunakan adalah *Wireshark* 4.2.4.

4.2 Akses *Website*

Dalam penelitian ini, peneliti menginisiasi dua skenario untuk memperluas cakupan analisis.

1. Pada *website Repository* UNHI

Menggunakan informasi pada akun berikut :

Username : ramandabayu04@gmail.com

Password : admin1234567890

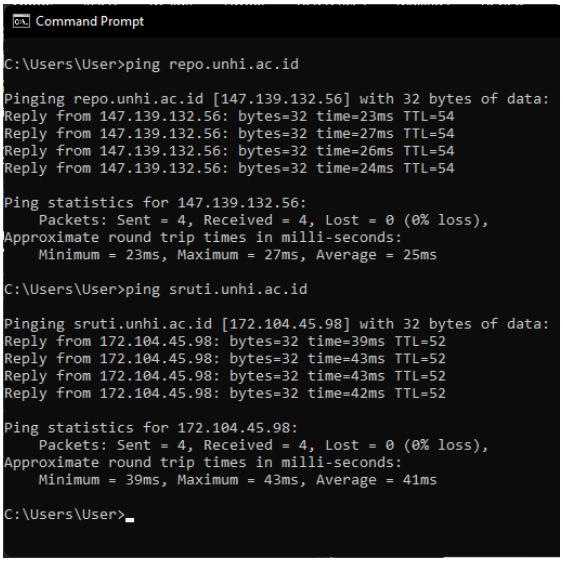
2. Pada *website SRUTI* UNHI

Menggunakan informasi pada akun berikut :

Username : 2003020015

Password : Password *SRUTI* 2020

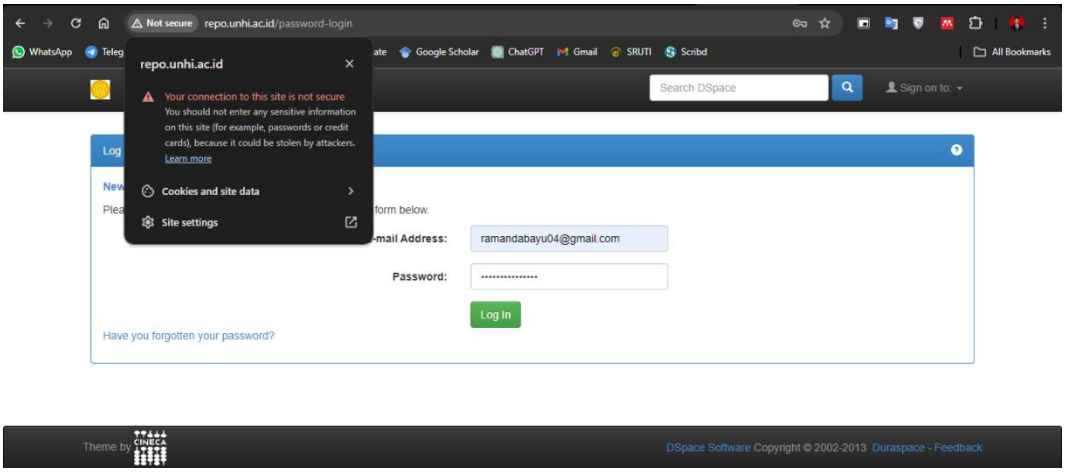
Gambar 4 menampilkan proses *PING* pada *website Repository* UNHI dan *SRUTI* UNHI melalui Command Prompt. Adapun *PING* dari kedua *website* tersebut yaitu: *Repository* UNHI dengan *PING* 147.139.132.56 dan *SRUTI* UNHI dengan *PING* 172.104.45.98.



Gambar 4 Proses *PING* Pada *CMD*

4.3 *Capturing Repository* UNHI

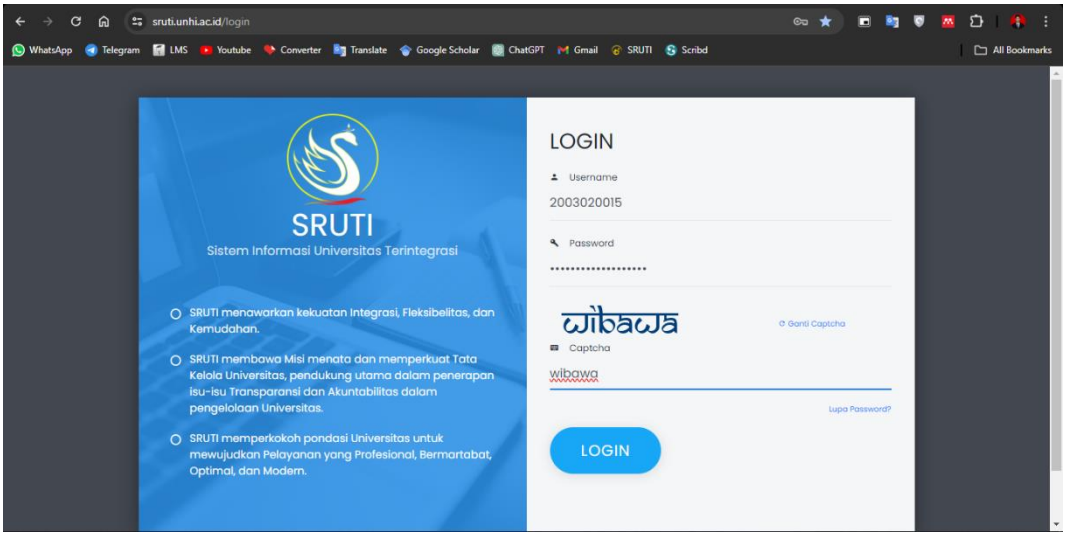
Pada Gambar 5, setelah melakukan "*Start Capturing Packets*" pada aplikasi *Wireshark*, lakukan akses *login* pada *website Repository* UNHI pada alamat *http://repo.unhi.ac.id/password-login* dengan memasukkan data sebagai berikut *username*: ramandabayu04@gmail.com dan *password*: admin1234567890. Jika sudah berhasil login pada *website Repository* UNHI, lakukan "*Stop Capturing*" pada aplikasi *Wireshark*.



Gambar 5 Halaman *Login Repository* UNHI

4.4 *Capturing SRUTI* UNHI

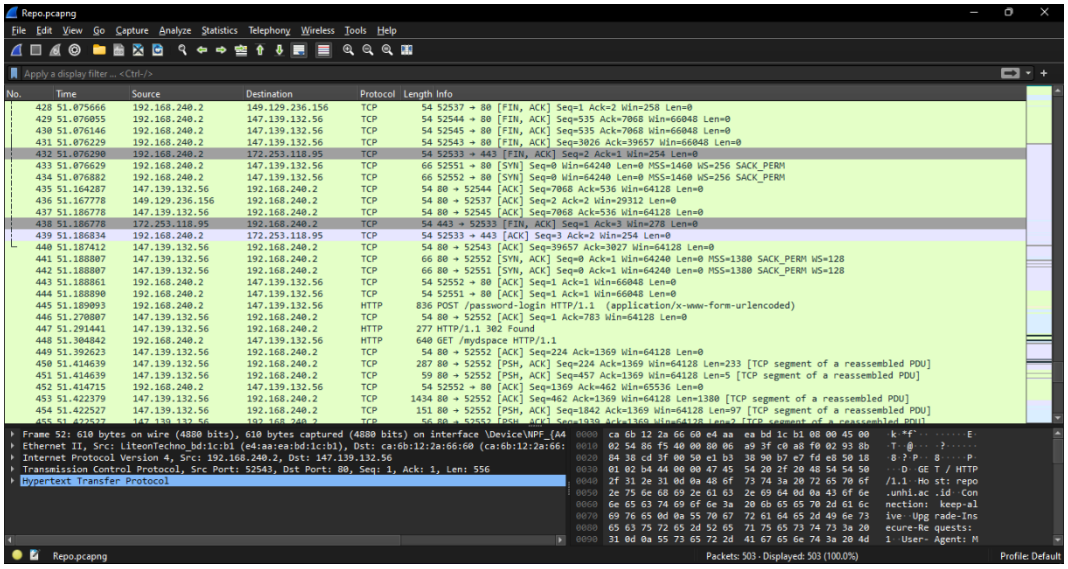
Pada Gambar 6, *login* ke *website SRUTI* UNHI dengan menekan "*Start Capturing Packets*" pada aplikasi *Wireshark*, lakukan akses *login* pada *website SRUTI* UNHI pada alamat *https*://*sruti.unhi.ac.id/login* dengan memasukkan data sebagai berikut *username*: 2003020015 dan *password*: *Password SRUTI* 2020. Jika sudah berhasil login pada *website Repository* UNHI, lakukan "*Stop Capturing*" pada aplikasi *Wireshark*.



Gambar 6 Halaman *Login SRUTI* UNHI

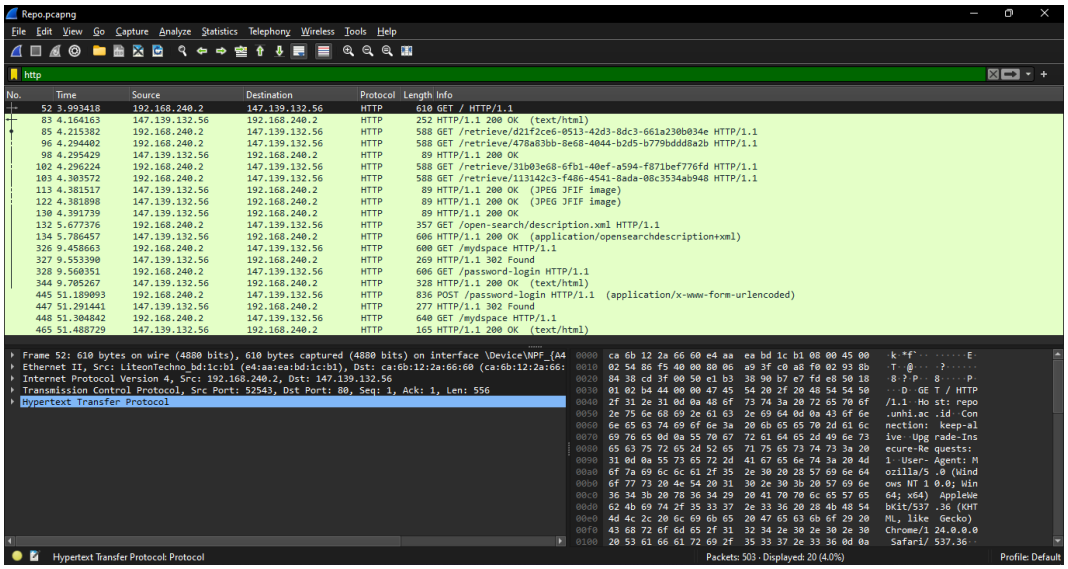
4.5 Analisis Keamanan Data *Repository* UNHI

Gambar 7 menampilkan hasil rekaman dari serangan packet *sniffing* menggunakan perangkat lunak *Wireshark* pada *website Repository* UNHI. Rekaman ini mencatat semua aktivitas yang terjadi dalam jaringan.



Gambar 7 Hasil Rekaman Paket Data Pada *Website Repository* UNHI

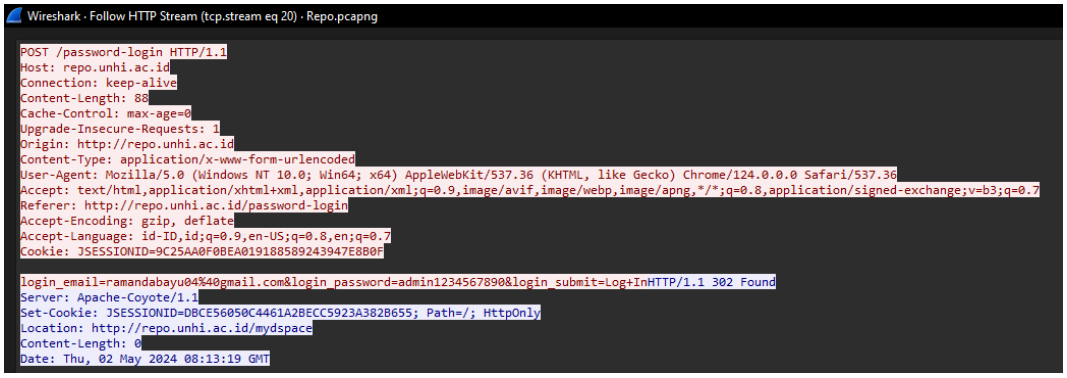
Untuk melakukan analisis paket data, informasi detail dari setiap paket bisa dilihat dalam panel detail. Dalam penelitian ini yang berfokus pada analisis keamanan *website*, peneliti melakukan penyaringan lanjutan dengan menggunakan perintah "*HTTP*" dalam Aplikasi *Wireshark* pada Gambar 8. Hal ini bertujuan untuk menampilkan paket-paket yang menggunakan protokol *HTTP*.



Gambar 8 Hasil Penyaringan Paket Data *Repository* UNHI

Gambar 8 menampilkan paket data dari *web Repository* UNHI yang menggunakan protokol *HTTP*. Setelah proses penyaringan (*filtering*) protokol *HTTP*, tersisa 19 paket data yang diperlihatkan. Dalam menu "Info", terdapat informasi, yaitu *GET*, *HTTP*/1.1, dan *POST*. Pada data *POST* terdapat informasi seperti alamat IP 192.168.240.2 sebagai *source* dan 147.139.132.56 sebagai *destination*.

Untuk melakukan analisis lebih lanjut terhadap paket data diatas, dilakukan dengan mengklik kanan pada paket data yang terdapat dalam panel daftar paket, lalu memilih opsi "*Follow HTTP Stream*". Tampilan rincian paket data protokol *HTTP* yang memiliki informasi "*POST*" diperlihatkan pada Gambar 9.

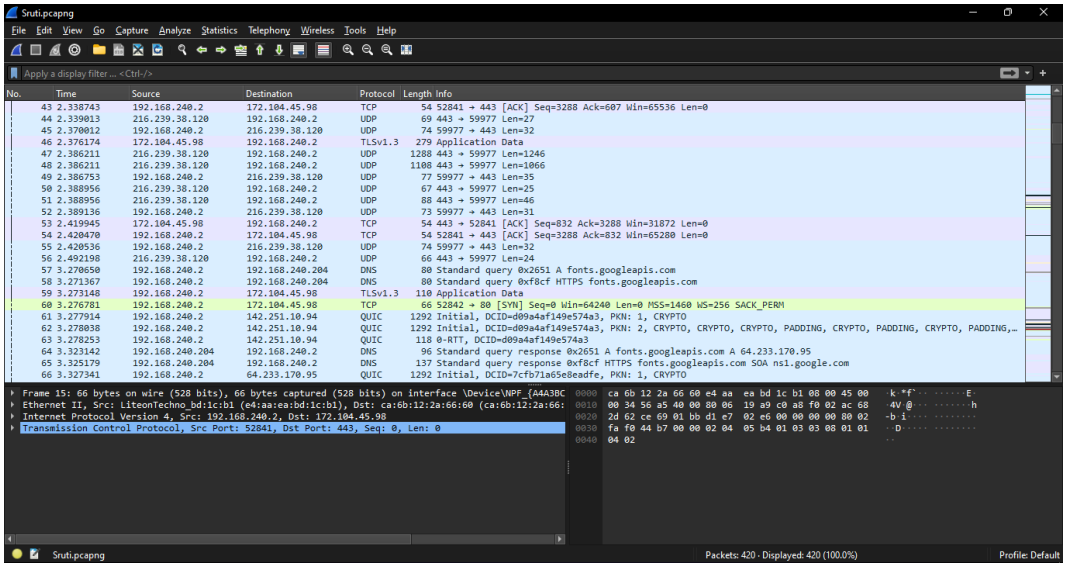


Gambar 9 Detail Paket Data *POST Repository* UNHI

Gambar 9 menunjukkan bahwa dalam detail paket data *POST* pada protokol *HTTP*, terdapat 2 (dua) warna teks yang memiliki makna berbeda. Teks berwarna merah adalah permintaan (*request*) *HTTP*, sementara teks berwarna biru adalah respons (*response*) *HTTP*. Salah satu paket data dengan informasi *POST* memuat berbagai data, termasuk informasi sensitif seperti nama pengguna (*username*) dan kata sandi (*password*) yang digunakan.

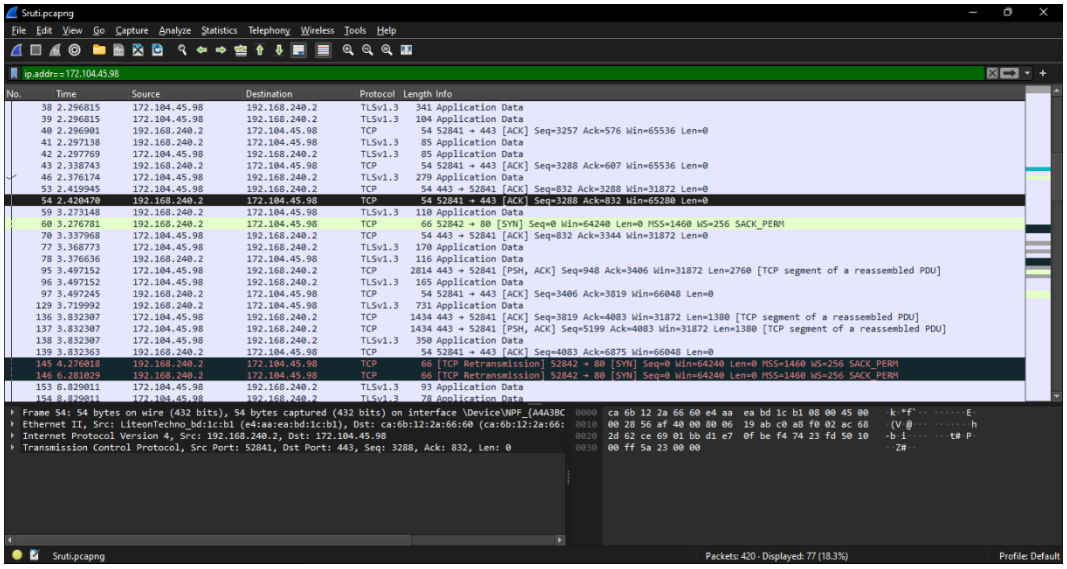
4.6 Analisis Keamanan Data *SRUTI* UNHI

Gambar 10 menampilkan hasil *capturing* dari serangan packet *sniffing* menggunakan perangkat lunak *Wireshark* pada *website SRUTI*. Rekaman ini mencatat semua aktivitas yang terjadi dalam jaringan.



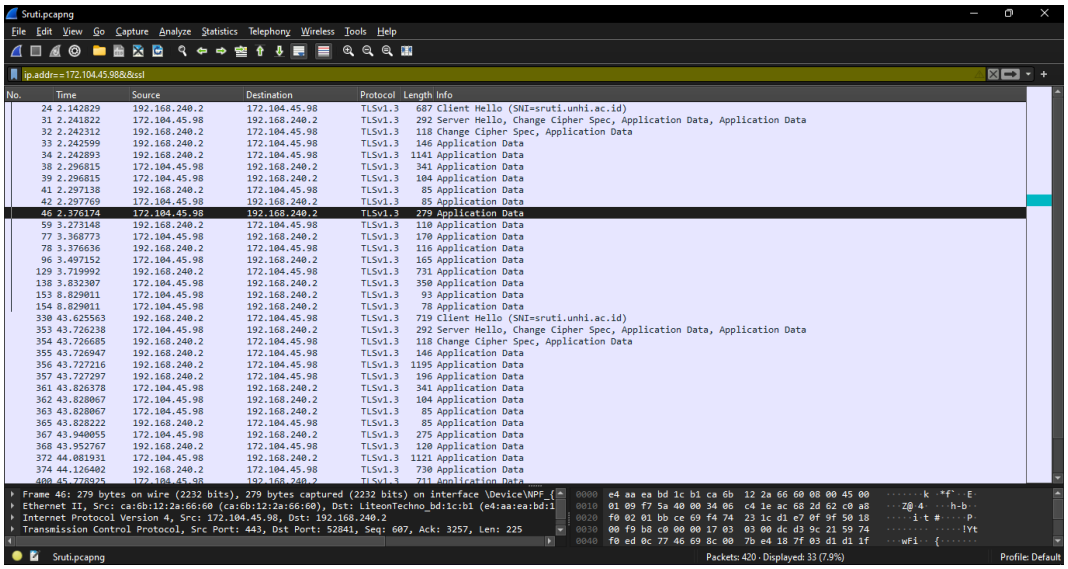
Gambar 10 Hasil Rekaman Paket Data pada *website SRUTI* UNHI

Untuk melakukan analisis paket data, informasi detail dari setiap paket bisa dilihat dalam panel detail. Dalam penelitian ini yang berfokus pada analisis keamanan *website*, peneliti melakukan penyaringan lanjutan dengan menggunakan perintah “ip.addr==172.104.45.98” pada *Wireshark*. Berikut salah satu tampilan detail paket data pada Gambar 11.



Gambar 11 Hasil Penyaringan Paket Data *SRUTI* UNHI

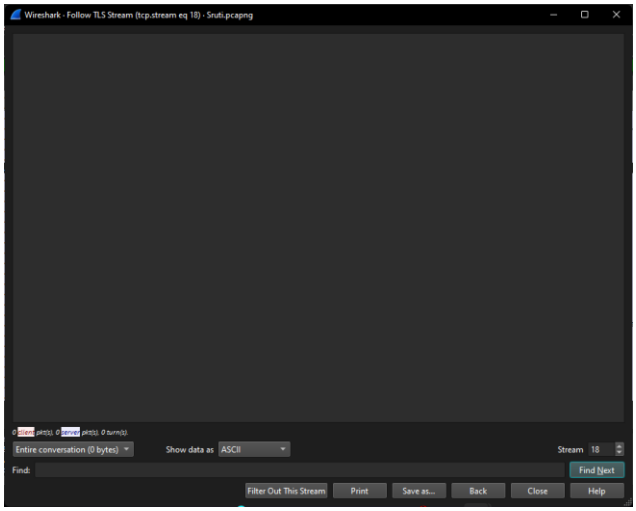
Pada Gambar 11 menampilkan seluruh paket data yang memiliki *IP Address* 172.104.45.98 yang terdapat pada *Source* maupun pada *Destination*. Dari 450 paket data yang diperlihatkan terdapat 2 (dua) jenis protokol yang dipakai yaitu protokol *Transport Layer Security* (*TLS*) dan *Transmission Control Protocol* (*TCP*). Koneksi *internet* lebih dominan memakai protokol *TCP* membuat hasilnya lebih banyak paket *TCP* yang terlihat.



Gambar 12 Paket Data *SRUTI* UNHI dengan Protokol *TLS*

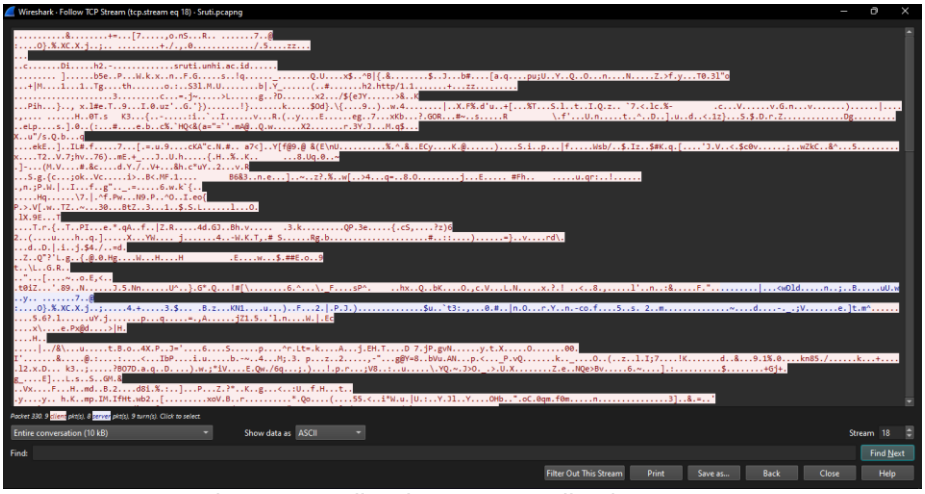
Dalam penelitian ini yang berkaitan dengan analisis keamanan *website*, peneliti melakukan penyaringan lebih lanjut dengan memasukkan perintah "ip.addr==172.104.45.98&&SSL" pada *Wireshark*. Ini bertujuan untuk menampilkan paket-paket yang terkait dengan protokol *SSL*, seperti yang ditunjukkan dalam Gambar 12.

Untuk menganalisis lebih lanjut, pilih paket data yang akan dianalisis dengan mengklik kanan dan kemudian pilih opsi "*Follow SSL Stream*". Tampilan rincian data paket untuk protokol *TLS* yang mengandung informasi *Application Data* pada Gambar 13.



Gambar 13 Detail Paket Data *Application Data TLS*

Gambar 13 menampilkan tampilan dari hasil "*Follow TCP Stream*" dan "*Follow SSL Stream*" dari informasi yang telah dipilih. Namun, detail paket data protokol *TLS* yang ada pada gambar tersebut, tidak ada informasi yang ditemukan.



Gambar 14 Detail Paket Data *Application Data TCP*

Gambar 14 merupakan analisis pada paket data yang sama melalui cara mengklik kanan pada paket data yang akan dianalisa dan memilih opsi "*Follow TCP Stream*". Namun, dari panel "*Follow TCP Stream*", peneliti kesulitan menganalisis informasi karena data yang dikirim telah dienkripsi.

5. Kesimpulan

Berdasarkan penjelasan sebelumnya, dapat disimpulkan hal-hal berikut:

1. Proses penyadapan (*sniffing process*) dapat dilakukan pada *website Repository* UNHI dan *website SRUTI* UNHI dengan menggunakan aplikasi *Wireshark*. Proses ini melibatkan perekaman (*capturing*) lalu lintas jaringan yang mengalir melalui jaringan *mobile hotspot*. Aplikasi *Wireshark* digunakan untuk menangkap dan menganalisis paket data yang dikirim dan diterima oleh *website Repository* UNHI dan *website SRUTI* UNHI. *Wireshark* merekam setiap paket data yang melewati jaringan *mobile hotspot*, memungkinkan peneliti untuk melihat dan menganalisis isi dari paket-paket tersebut.
2. Hasil analisis menunjukkan perbedaan dalam tingkat keamanan data antara *website Repository* UNHI dan *website SRUTI* UNHI. Pada *website Repository* UNHI yang menggunakan *HTTP* terbukti rentan terhadap serangan *sniffing*, aplikasi *Wireshark* berhasil menangkap dan menganalisis paket data yang dikirim antara pengguna dan *server*, termasuk informasi sensitif seperti *username* dan *password*. Hal ini menunjukkan

bahwa protokol *HTTP* tidak menyediakan enkripsi data, sehingga tidak optimal dalam melindungi data dari ancaman *sniffing*. Sebaliknya, pada *website SRUTI* UNHI yang menggunakan protokol *HTTPS* memiliki tingkat keamanan yang lebih tinggi. Informasi yang diperoleh dari pelacakan *IP* halaman yang dikunjungi hanya mencakup *IP* asal dan tujuan, serta server dan port yang digunakan untuk komunikasi. Jumlah paket data yang melewati jaringan dapat diketahui, namun isi paket tersebut tidak dapat dibaca karena sudah terenkripsi. Data yang dikirim dienkripsi dengan *SSL*/*TLS*, memberikan lapisan perlindungan tambahan yang membuatnya sulit untuk diakses, sehingga meskipun paket data dapat ditangkap oleh *Wireshark*, isi dari paket tersebut tidak dapat dibaca. Penelitian ini menunjukkan bahwa penggunaan protokol *HTTPS* secara signifikan meningkatkan keamanan data pada *website* dibandingkan dengan penggunaan protokol *HTTP*. Hal ini ditunjukkan dari hasil analisis data yang menangkap dan membandingkan paket data yang dikirim melalui kedua protokol tersebut.

Daftar Pustaka

[1] Majid A, Purwanto TD, Analisis Dan Monitoring Sniffing Paket Data Jaringan Lokal Bps Sumseldengan Network Analyzer Wireshark, Seminar Hasil Penelitian Vokasi (SEMHAVOK). 2021; 03(1): 102-109.

[2] Huzaeni F, Gunawan I, Cahya D, Yanti M, Krisdayanti N. Analisis Keamanan Data Pada Website Dengan Wireshark. JES (Jurnal Elektro Smart). 2021; 1(1): 13-17.

[3] Picard M. Kebalian: Konstruksi Dialogis Identitas Bali. Kepustakaan Populer Gramedia. 2020.

[4] Universitas Hindu Indonesia. Editors. Pedoman Akademik Universitas Hindu Indonesia Tahun 2023/2024. Denpasar: Universitas Hindu Indonesia; 2023.

[5] Alfian DK. Apa Perbedaan HTTP dan HTTPS? Lengkap Beserta Penjelasannya - Dicoding Blog. https://www.dicoding.com/blog/perbedaan-HTTP-dan-HTTPS/, diakses tanggal 24 Juni 2020.

[6] Iskandar A, Geni BY, Prabiantissa CN, Kurnaedi D, Wahyuddin S, Samosir K, Supriyadi A. Pengantar Jaringan Komputer. GET Press; 2022.

[7] Arumawan DP. Upaya Kepolisian Dalam Rangka Menjaga Keamanan Sistem M-Banking Terhadap Ancaman Serangan Siber Melalui Teknik Scamming. Masters Thesis Universitas Lampung. 2023.

[8] Windra IY. Simulasi Perancangan Infrastruktur Jaringan Komputer Pada Institut Teknologi Keling Kumang Menggunakan Pendekatan Network Development Life Cycle (NDLC). TAWAK: Jurnal Hunatech. 2022; 1(2).

[9] Faaizah N. Apa Saja Contoh Data Primer? Berikut Contoh dan Metode Pengumpulannya. Detik.Com.https://www.detik.com/edu/detikpedia/d-7034653/apa-saja-contoh-data-primer-berikut-contoh-dan-metode-pengumpulannya, diakses tanggal 14 November 2023.

[10] Sarjana N. Definisi Data Sekunder dan Cara Memperolehnya. Detik.Com. https://www.detik.com/edu/detikpedia/d-6843072/definisi-data-sekunder-dan-cara-memperolehnya, diakses tanggal 26 Juni 2023.

[11] Naim F, Saedudin RR, Hediyanto UYK. Analysis of Wireless and Cable Network Quality-of-Service Performance at Telkom University Landmark Tower Using Network Development Life Cycle (NDLC) Method. JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika). 2022; 7(4): 1033–1044.

[12] Rivai MR. Penerapan Algoritma Rivest Shamir Adleman pada IPSEC (Internet Protocol Security) untuk Router dalam Perluasan Jaringan. Repository Universitas Binaniaga Indonesia. 2022.

[13] Jamaluddin, H., & Suaeb, N. F. (2018). Analisis Keamanan Website terhadap Sniffing Process pada Jaringan Nirkabel Menggunakan Aplikasi Wireshark (Studi Kasus: Simak Unismuh).

[14] Farhan RM, Hendita G, Kusuma A. Teknik Sniffing Jaringan Menggunakan Wireshark. Journal of Informatics and Advanced Computing (JIAC). 2023; 4(1).

[15] Syafnidawaty. APA ITU REPOSITORY? - UNIVERSITAS RAHARJA. Universitas Raharja. https://raharja.ac.id/2020/11/13/apa-itu-Repository/, diakses tanggal 13 November 2020.

[16] Hanipah R, Dhika H. Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark. DoubleClick: Journal of Computer and Information Technology. 2020; 4(1): 11-23.