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} ^aProgram Studi Sistem Informasi, Fakultas Teknologi Informasi dan Sains, Universitas Hindu Indonesia, Indonesia e-mail: ¹ramandabayu04@gmail.com, ²andyasmarajaya@unhi.ac.id, ³iknadijaya@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 memggunakan 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.

 Pada website Repository UNHI Menggunakan informasi pada akun berikut : Username : ramandabayu04@gmail.com Password : admin1234567890
 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*.

← → C ^a	ଲି 🖌	Not secure repo.unhi.ac.id/password-login	n ate	🔶 Google Scholar	ChatGPT	M Gmail	🕝 SRUTI	🕃 Scribd	ං ද <u>ා</u>		N V	8		Bookmarks
	Log New Plea	Your connection to this site is not secure. You should not enter any sensitive informatio on this site for example, passwords or credit cardly, because it could be stolen by attacker <u>Learn more</u> Cockies and site data Site settings	on 3. 2 form -mai	below. Address:	ramandabayu 	04@gmail.c	om	Search DSpace		٩	L Sign	on to: •		
i i	Theme by							DSpace Software Co	pyright © 200	02-2013	Duraspace	- Feedt	ack	

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.

🚄 Repo.pcapng	-	o ×
Eile Edit View Go Capture Analyze Statistics Telephony Wire	eless Iools Help	
4 🗆 4 🙆 🖿 🖻 🖄 🖻 🎗 👄 🔿 🗛 🔳	= 0 0 0 m	
Apply a display filter < Ctrl-/>		• • •
No. Time Source Destination	Protocol Length Info	A
428 51.075666 192.168.240.2 149.129.236.1	56 TCP 54 52537 → 80 [FIN, ACK] Seg=1 Ack=2 Win=258 Len=0	
429 51.076055 192.168.240.2 147.139.132.5	6 TCP 54 52544 → 80 [FIN, ACK] Seg=535 Ack=7068 Win=66048 Len=0	
430 51.076146 192.168.240.2 147.139.132.5	6 TCP 54 52545 → 80 [FIN, ACK] Seq=535 Ack=7068 Win=66048 Len=0	
431 51.076229 192.168.240.2 147.139.132.5	6 TCP 54 52543 → 80 [FIN. ACK] Seq=3026 Ack=39657 Win=66048 Len=0	
432 51.076290 192.168.240.2 172.253.118.9	5 TCP 54 52533 → 443 [FIN, ACK] Seq=2 Ack=1 Win=254 Len=0	
433 51.076629 192.168.240.2 147.139.132.5	6 TCP 66 52551 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	
434 51.076882 192.168.240.2 147.139.132.5	6 TCP 66 52552 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	
435 51.164287 147.139.132.56 192.168.240.2	TCP 54 80 → 52544 [ACK] Seq=7068 Ack=536 Win=64128 Len=0	
436 51.167778 149.129.236.156 192.168.240.2	TCP 54 80 → 52537 [ACK] Seq=2 Ack=2 Win=29312 Len=0	
437 51.186778 147.139.132.56 192.168.240.2	TCP 54 80 → 52545 [ACK] Seq=7068 Ack=536 Win=64128 Len=0	
438 51.186778 172.253.118.95 192.168.240.2	TCP 54 443 → 52533 [FIN, ACK] Seq=1 Ack=3 Win=278 Len=0	
439 51.186834 192.168.240.2 172.253.118.9	5 TCP 54 52533 + 443 [ACK] Seq=3 Ack=2 Win=254 Len=0	
440 51.187412 147.139.132.56 192.168.240.2	TCP 54 80 → 52543 [ACK] Seq=39657 Ack=3027 Win=64128 Len=0	
441 51.188807 147.139.132.56 192.168.240.2	TCP 66 80 → 52552 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1380 SACK_PERM WS=128	
442 51.188807 147.139.132.56 192.168.240.2	TCP 66 80 → 52551 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1380 SACK_PERM WS=128	
443 51.188861 192.168.240.2 147.139.132.5	6 TCP 54 52552 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0	
444 51.188890 192.168.240.2 147.139.132.5	6 TCP 54 52551 + 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0	
445 51.189093 192.168.240.2 147.139.132.5	6 HTTP 836 POST /password-login HTTP/1.1 (application/x-www-form-urlencoded)	
446 51.270807 147.139.132.56 192.168.240.2	TCP 54 80 → 52552 [ACK] Seq=1 Ack=783 Win=64128 Len=0	
447 51.291441 147.139.132.56 192.168.240.2	HTTP 277 HTTP/1.1 302 Found	
448 51.304842 192.168.240.2 147.139.132.5	6 HTTP 640 GET /mydspace HTTP/1.1	
449 51.392623 147.139.132.56 192.168.240.2	ICP 54 80 + 52552 [ACK] Seq=224 ACK=1369 Win=64128 Len=0	
450 51.414639 147.139.132.56 192.168.240.2	ICP 287 80 + 52552 [PSH, ACK] Seq=224 ACK=1569 Win+64128 Len=253 [ICP segment of a reassembled PDU]	
451 51.414039 147.139.152.50 192.108.240.2	1CP 59 60 + 52552 [PSn, ACK] Seq=457 ACK=1569 Win=64126 Len=5 [ICP segment of a reassembled Pb0]	
452 51.414/15 192.168.240.2 147.139.132.5	6 ICP 54 52552 + 80 [ACK] Seq=1369 ACK=402 Win=65536 Len=0	
453 51.4223/9 147.139.132.56 192.168.240.2	ICP 1434 80 + 52552 [ACK] Seq=462 ACK=1599 WIN=64128 Len=1380 [ICP segment of a reassembled PUU]	
454 51.422527 147.139.132.50 192.100.240.2	TCP 101 00 + 52552 [PSH, ACK] Seq=1042 ACK=1309 Win=04120 Len=97 [TCP segment of a reassembled PDU]	-
Entre 52: 610 huter on vine (4000 hits) 610 huter and		
Frame 52: 610 bytes on wire (4660 bits), 610 bytes capital for the second state of	(u) = (u)	
Fullement II, Sic. Liteometino_bullet.bi (e4.88.88.00.10)		
 Transmission Control Protocol Sec Port: 52543 Det Por 	117, 137, 137, 137, 100 00 10 100 00 10 100 00 10 100 100	
Hypertext Transfer Protocol	0040 2 f 31 2a 31 00 00 48 6f 73 74 3 20 77 65 70 6f /1 1 the ft range	
in a second se	0050 2 27 55 66 68 69 26 61 63 26 64 64 84 33 65 66 unbit ac id. Con	
	9960 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c pection: keen-al	
	0070 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 ive Upg rade-Ins	
	0000 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 ecure-Re guests:	
4	▶ 0090 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 1 User- Agent: M	
Seno prappo	Parkets: 503 - Displayert: 503 (100.0%)	Profile: Default
- Incholacobuld	Tackets 303 - Displayed, 303 (1000 A)	Contraction of the second second

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*.

Repo.pcapng					– o ×
<u>File Edit View Go</u>	<u>Capture</u> <u>A</u> nalyze <u>S</u> tatistic	cs Telephony <u>W</u> ireless	<u>Tools</u> <u>H</u> elp		
/ II # @ 🖿 H	🗎 🔀 😫 🍳 👄 🔿	🖻 🛉 🕹 🔳 🔳 🤊	ଇ ଇ ଇ ।		
http					
No. Time	Source	Destination	Protocol	Length Info	
52 3.993418	192.168.240.2	147.139.132.56	HTTP	610 GET / HTTP/1.1	·
T 83 4.164163	147.139.132.56	192.168.240.2	HITP	252 HIP/1.1 200 OK (Text/ntml)	
96 4.294402	192.168.240.2	147.139.132.56	HTTP	588 GFT /retrieve/478a83bb-8e68-4044-b2d5-b779bddd8a2b HTTP/1.1	
98 4,295429	147,139,132,56	192,168,240,2	HTTP	89 HTTP/1.1 200 OK	
102 4.296224	192.168.240.2	147.139.132.56	HTTP	588 GET /retrieve/31b03e68-6fb1-40ef-a594-f871bef776fd HTTP/1.1	
103 4.303572	192.168.240.2	147.139.132.56	HTTP	588 GET /retrieve/113142c3-f486-4541-8ada-08c3534ab948 HTTP/1.1	
113 4.381517	147.139.132.56	192.168.240.2	HTTP	89 HTTP/1.1 200 OK (JPEG JFIF image)	
122 4.381898	147.139.132.56	192.168.240.2	HTTP	89 HTTP/1.1 200 OK (JPEG JFIF image)	
130 4.391/39	147.139.132.56	192.168.240.2	HITP	89 HTTP/1.1 200 OK	
134 5 786457	147 139 132 56	192 168 249 2	HTTP	606 HTTP/1 1 200 0K (application/opensearchdescription+yml)	
326 9,458663	192.168.240.2	147.139.132.56	HTTP	600 GET /mydsoace HTTP/1.1	
327 9.553390	147.139.132.56	192.168.240.2	HTTP	269 HTTP/1.1 302 Found	
328 9.560351	192.168.240.2	147.139.132.56	HTTP	606 GET /password-login HTTP/1.1	
344 9.705267	147.139.132.56	192.168.240.2	HTTP	328 HTTP/1.1 200 OK (text/html)	
445 51.189093	192.168.240.2	147.139.132.56	HTTP	836 POST /password-login HTTP/1.1 (application/x-www-form-urlencoded)	
447 51.291441	147.139.132.56	192.168.240.2	HTTP	277 HTTP/1.1 302 Found	
440 51.504042	192.100.240.2	102 168 240 2	NTTP	040 0CI / myospace niiP/iii	
403 31.400723	147.139.132.30	192.100.240.2		105 mm//1.1 200 0K (CEXE/ITCHI)	
Ecame 52: 610 byte	s on wire (4880 bits). 610 bytes cantured	(4880 bits) on interface \Device\NPE {44, 0000, ca 6b 12 2a 66 60 e4 aa, ea bd 1c b1 08 00 45 00	k.*f`
Ethernet II, Src:	LiteonTechno bd:1c:b.	1 (e4:aa:ea:bd:1c:b1)	. Dst: ca:6	b:12:2a:66:60 (ca:6b:12:2a:66: 0010 02 54 86 f5 40 00 80 06 a9 3f c0 a8 f0 02 93 8b	Τ
Internet Protocol	Version 4, Src: 192.	168.240.2, Dst: 147.1	39.132.56	0020 84 38 cd 3f 00 50 e1 b3 38 90 b7 e7 fd e8 50 18	8-? P 8P-
Transmission Contr	rol Protocol, Src Port	t: 52543, Dst Port: 8	0, Seq: 1,	Ack: 1, Len: 556 0030 01 02 b4 44 00 00 47 45 54 20 2f 20 48 54 50	· D· GE T / HTTP
Hypertext Transfer	Protocol			0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 72 65 70 6f /	1.1 Ho st: repo
				0050 2e 75 6e 68 69 2e 61 63 2e 69 64 0d 0a 43 6f 6e .	unhi.ac .id Con
				0050 be b5 b3 /4 b9 bt be 3a 20 bb b5 b5 /0 2d b1 bc n	ection: keep-al
					cure-Re quests
				0000 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 1	User- Agent: M
				00a0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 o	zilla/5 .0 (Wind
				00b0 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e o	ws NT 1 0.0; Win
				00c0 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 6	4; x64) AppleWe
				00d0 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 b	Kit/537 .36 (KHT
				0000 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 M	L, like Gecko)
-				0010 43 66 72 67 66 65 27 31 32 34 26 30 26 30 26 30 C	Safari/ 537 36
· · · · · · · · · · · · · · · · · · ·	- D			0 0000 20 33 01 00 01 72 09 21 35 35 37 22 33 30 00 0a	
Hypertext Transf	er Protocol: Protocol			Packets: 503 - Displayed: 20 (4.0%)	Profile: Default

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.

🚄 Wireshark - Follow HTTP Stream (tcp.stream eq 20) - Repo.,pcapng
POST /password-login HTTP/1.1
Host: repo.unhlac.id
Contection: Keep-allve
Upgrade-Insecure-Requests: 1
Origin: http://repo.unhi.ac.id
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://repo.unh.ac.1d/password-login
Accept-Encooling: gzip, deflate
Cockie: ISESSIONTD=9C/SAA04F0FEA019188589243947E886F
login_email=ramandabayu04%40gmail.com&login_password=admin1234567890&login_submit=Log+InHTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=DBCE56050C4461A2BECC5923A3828655; Path=/; HttpOnly
Location: http://repo.unhi.ac.id/mydspace
Date: The gala we and estate of
Date: Inu, 02 may 2024 00:10:10 umi

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.

💋 Sruti.pcapng				– Ø ×
<u>File Edit View Go C</u>	apture <u>A</u> nalyze <u>S</u> tatistic	s Telephony <u>W</u> ireless <u>T</u> e	ools <u>H</u> elp	
⊿ 🗆 🔬 🎯 🖿 🖬	1 🔀 🖻 🍳 🗢 🔿	🖄 🛉 🕹 🔳 🔳 🔍		
Apply a display filter				
		D <i>K K</i>	a	
No. lime	source	Destination	Protocol	
43 2.338/43	192.168.240.2	1/2.104.45.98	TCP	54 52841 + 443 [ACK] SEq=3288 ACK=607 Win=65536 Len=0
44 2.339013	102 168 240 2	192.100.240.2	UDP	03 445 + 3337/ Lem=2/
45 2.370012	192.168.240.2	216.239.38.120	UDP TLCUIL D	/4 599/1 + 443 Len=32
40 2.376174	172.104.45.96	192.108.240.2	11501.5	2/9 Application Data
47 2.300211	216.239.30.120	192.100.240.2	UDP	1200 445 * 5397/ L01=1240
40 2 296752	102 168 240 2	216 220 22 120	UDD	77 5077 + 43 / 0777 = 25
49 2.300/33	192.100.240.2	210.259.50.120	UDP	// 399// + 443_LET=33
50 2.300930	210.239.30.120	192.100.240.2	UDP	07 445 7 53577 L01=25
51 2.380530	102 169 240 2	216 220 28 120	UDD	00 443 7 55577 LCII-40
52 2.309130	172 104 45 09	103 168 349 3	TCD	53 33377 + HHS LEHIST 54 443 - 513441 [ArV] 5931 A-4-2309 [Jan-21973]0
55 2.419949	102 168 240 2	172 104 45 02	TCD	54 TES 4 5 2011 [Rec] 300-052 Actor 2020 Ministration Come
55 2 420536	192 168 240 2	216 239 38 120	LIDP	74 50977 + 43 [en-3]
56 2 492198	216, 239, 38, 129	192,168,240,2	UDP	66 443 + 5977 Len=24
57 3 279659	192 168 249 2	192 168 249 294	DNS	80 Standard query 0/2651 A fonts googleanis com
58 3 271367	192 168 240 2	192 168 240 204	DNS	80 Standard query 0x58cf HTDS fonts googlegatis com
59 3 273148	192 168 249 2	172 104 45 98	TISV1 3	110 Application Data
69 3 276781	192 168 240 2	172 104 45 98	TCP	66 52842 + 80 [SVN] Seg-0 Win-64240 Len-0 MSS-1460 WS-256 SACK DEDM
61 3 277914	192 168 240 2	142 251 10 94	OUTC	1292 Taitial DCTm+d094af14957433 PKN-1 CEVPTO
62 3 278938	192 168 249 2	142 251 10 94	OUTC	1202 Trittial DCTD-d0a4af140a574a3 DKN-2 CDVDTO CDVDTO CDVDTO DADDING CDVDTO DADDING
63 3 278253	192 168 240 2	142 251 10 94	OUTC	118 A.PTT DCD-d03daf140e5743
64 3.323142	192, 168, 249, 294	192,168,240,2	DNS	96 Standard query resonance 0x2651 A fonts googleanis com A 64 233 170 95
65 3, 325179	192.168.240.204	192.168.240.2	DNS	137 Standard query response 0x58cf HTDPS fonts googleanis.com SDA ns1.google.com
66 3.327341	192.168.240.2	64.233.170.95	QUIC	1292 Initial, DCID=7cfb7la65e8eadfe, PKN: 1, CRYPTO
▶ Frame 15: 66 bytes	on wire (528 bits).	66 bytes captured (528	3 bits) on	interface \Device\NPF {A443BC 0000 ca 6b 12 2a 66 60 e4 aa ea bd 1c b1 08 00 45 00 ··k·*f`······E·
Ethernet II, Src:	LiteonTechno_bd:1c:b1	(e4:aa:ea:bd:1c:b1),	Dst: ca:6	b:12:2a:66:60 (ca:6b:12:2a:66: 0010 00 34 56 a5 40 00 80 06 19 a9 c0 a8 f0 02 ac 68 4V @······h
Internet Protocol	Version 4, Src: 192.1	68.240.2, Dst: 172.104	1.45.98	0020 2d 62 ce 69 01 bb d1 e7 02 e6 00 00 00 00 80 02 -b i ····
Transmission Contr	ol Protocol, Src Port	: 52841, Dst Port: 443	3, Seq: 0,	0030 fa f0 44 b7 00 00 02 04 05 b4 01 03 03 08 01 01 ··D·····
				0040 04 02 ···
4				
🔵 🗹 Sruti.pcapng				Packets: 420 · Displayed: 420 (100.0%) Profile: Default

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.

🥖 Sruti.pcapng		- o ×
Eile Edit View Go Capture Analyze Statistics Telephony Wireless	Icols Help	
	<u>ର୍ର୍ର୍</u> ମ	
ip.addr==172.104.45.98		
No Time Source Destination	Protocal Leasth lafe	-
28 0 006915 170 104 45 08 100 168 040 0	Flotter Length Into	
39 2 296815 172 104 45 98 192 168 249 2	TISVI 3 JA Application bits	
40 2,296901 192,168,240,2 172,104,45,98	TCP 52841 + 443 [ACK] Seg=3257 Ack=576 Win=65536 Len=0	
41 2,297138 192,168,240,2 172,104,45,98	TLSv1.3 85 Application Data	
42 2.297769 172.104.45.98 192.168.240.2	TLSv1.3 85 Application Data	
43 2.338743 192.168.240.2 172.104.45.98	TCP 54 52841 → 443 [ACK] Seq=3288 Ack=607 Win=65536 Len=0	
46 2.376174 172.104.45.98 192.168.240.2	TLSv1.3 279 Application Data	
53 2.419945 172.104.45.98 192.168.240.2	TCP 54 443 → 52841 [ACK] Seq=832 Ack=3288 Win=31872 Len=0	
54 2.420470 192.168.240.2 172.104.45.98	TCP 54 52841 → 443 [ACK] Seq=3288 Ack=832 Win=65280 Len=0	
59 3.273148 192.168.240.2 172.104.45.98	TLSv1.3 110 Application Data	
60 3.276781 192.168.240.2 172.104.45.98	TCP 66 52842 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	
70 3.337968 172.104.45.98 192.168.240.2	TCP 54 443 → 52841 [ACK] Seq=832 Ack=3344 Win=31872 Len=0	
77 3.368773 172.104.45.98 192.168.240.2	TLSv1.3 170 Application Data	
78 3.376636 192.168.240.2 172.104.45.98	TLSv1.3 116 Application Data	
95 3.497152 172.104.45.98 192.168.240.2	TCP 2814 443 + 52841 [PSH, ACK] Seq=948 Ack=3406 Win=31872 Len=2760 [TCP segment of a reassembled PDU]	
90 5.497152 172.104.45.96 192.106.240.2		
97 5.497245 192.100.240.2 172.104.45.90 120 2 710002 102 168 240 2 172 104 45 08	TLP 34 32041 7 445 [ALK] SEQ=3400 ALK=3013 WIN=00046 LEN=0	
125 3.715552 152.100.240.2 172.104.45.50 136 3.833267 173.104.45.09 103.169.340.3	TCD 1424 442 - 52841 [CACK] Sec.2010 Ack-4002 [No.21072 [co.1200 [TCD compost of a consecubled DNI]	
137 3 933397 172 104 45 09 102 169 240 2	TCP 1434 443 - 52041 [ACK] Seq 5100 Ack=4003 Wiles2002 Lefe12300 [TCP segment of a reassembled PD0]	
138 3.832307 172.104.45.98 192.168.240.2	TISV1.3 359 Application Data	
139 3.832363 192.168.249.2 172.104.45.98	TCP 54 52841 + 443 [ACK] Seg=4083 Ack=6875 Win=66048 Len=0	
145 4.276018 192.168.240.2 172.104.45.98	TCP 66 [TCP_Retransmission] 52842 → 80 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	
146 6.281029 192.168.240.2 172.104.45.98	TCP 66 [TCP Retransmission] 52842 → 80 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM	
153 8.829011 172.104.45.98 192.168.240.2	TLSv1.3 93 Application Data	
154 8.829011 172.104.45.98 192.168.240.2	TLSv1.3 78 Application Data	· · · · · · · · · · · · · · · · · · ·
Frame 54: 54 bytes on wire (422 bits), 54 bytes captured (ttheret II, Src: LiteonFebrua, bits): bits: (4:assesbit): bits internet Protocol Version 4, Src: 192.108,248.2, Dat: 172. Transmission Control Protocol, Src Port: 52843, Dat Port: 4	432 bitsi) on interface Ubevice.NVFF_LAAA3BC 0000 ca 6b 12 2a 66 60 44 aa ea bd 12 b 80 00 45 00 ik 4f ⁺ ···· E 19.4.5.56 194.5.56 194.5.56 45, Seq: 3288, Ack: 832, Len: 0 19.56 19.56 19.56 19.56 19.56 19.56 19.56 19.56 19.56 19.57	
🗢 🖉 Sruti.pcapng	Packets: 420 · Displayed: 77 (18.3%)	Profile: Defaul

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.

ddr==1/2.104.45.9	88c8cssl				× 🛋 -
Time		Destination	Protocol	anoth Info	
24 2 142829	192 168 249 2	172 104 45 98	TLSv1 3	687 Client Hello (SNT-cruiti unbi ac id)	
31 2.241822	172.104.45.98	192.168.240.2	TLSV1.3	292 Server Hello, Change Cinher Spec, Application Data, Application Data	
32 2.242312	192,168,240,2	172,104,45,98	TLSv1.3	118 Change Cipher Spec. Application Data	
33 2.242599	192,168,240,2	172.104.45.98	TLSv1.3	146 Application Data	
34 2.242893	192,168,240,2	172.104.45.98	TLSv1.3	141 Application Data	
38 2,296815	172.104.45.98	192,168,240,2	TLSv1.3	341 Application Data	
39 2.296815	172.104.45.98	192,168,240,2	TLSv1.3	104 Application Data	
41 2.297138	192,168,240,2	172,104,45,98	TLSv1.3	85 Application Data	
42 2.297769	172.104.45.98	192,168,240,2	TLSv1.3	85 Application Data	
46 2.376174	172.104.45.98	192.168.240.2	TLSv1.3	279 Application Data	
59 3.273148	192,168,240,2	172,104,45,98	TLSv1.3	110 Application Data	
77 3.368773	172.104.45.98	192.168.240.2	TLSv1.3	170 Application Data	
78 3.376636	192.168.240.2	172.104.45.98	TLSv1.3	116 Application Data	
96 3.497152	172.104.45.98	192.168.240.2	TLSv1.3	165 Application Data	
29 3.719992	192.168.240.2	172.104.45.98	TLSv1.3	731 Application Data	
38 3.832307	172.104.45.98	192.168.240.2	TLSv1.3	350 Application Data	
53 8.829011	172.104.45.98	192.168.240.2	TLSv1.3	93 Application Data	
54 8.829011	172.104.45.98	192.168.240.2	TLSv1.3	78 Application Data	
30 43.625563	192.168.240.2	172.104.45.98	TLSv1.3	719 Client Hello (SNI=sruti.unhi.ac.id)	
53 43.726238	172.104.45.98	192.168.240.2	TLSv1.3	292 Server Hello, Change Cipher Spec, Application Data, Application Data	
54 43.726685	192.168.240.2	172.104.45.98	TLSv1.3	118 Change Cipher Spec, Application Data	
55 43.726947	192.168.240.2	172.104.45.98	TLSv1.3	146 Application Data	
56 43.727216	192.168.240.2	172.104.45.98	TLSv1.3	1195 Application Data	
57 43.727297	192.168.240.2	172.104.45.98	TLSv1.3	196 Application Data	
61 43.826378	172.104.45.98	192.168.240.2	TLSv1.3	341 Application Data	
62 43.828067	172.104.45.98	192.168.240.2	TLSv1.3	104 Application Data	
63 43.828067	172.104.45.98	192.168.240.2	TLSv1.3	85 Application Data	
65 43.828222	192.168.240.2	172.104.45.98	TLSv1.3	85 Application Data	
67 43.940055	172.104.45.98	192.168.240.2	TLSv1.3	275 Application Data	
68 43.952767	192.168.240.2	172.104.45.98	TLSv1.3	120 Application Data	
72 44 091021	172.104.45.98	192.168.240.2	TLSv1.3	1121 Application Data	
72 44.001901	100 169 040 0	172 104 45 98	TLSv1 3	730 Application Data	
74 44.126402	192.100.240.2	2121201110100	1001010		

Gambar 12 Paket Data SRUT/ 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.

Wireshark - Follow ICP Stream (tcp.stream eq 18) - Srutupcaping	_	U	^
) 0g 8^5.		
Z.Q ⁻⁷ L.g.(<u>4</u> .0.HgHHH5.##E.O9			
t: · (
- t912'.89N	;B.	uU	4
եւու),Ֆ.Ж.Հ.ծ.,Ե.,	e.]t.	. m^	
	k	····+····	
D			
Packet 380 9 client pietoj. 9 surveja pietoj. 9 surveja cliek to select			
Entire conversation (10 kB) * Show data as ASCII *	Str	eam 18	٥
Find:		Find Ne	ext
Filter Out This Stream Print Seve as Back Cli	55 0	Help	

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

- 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-primerberikut-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-caramemperolehnya, 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.