

SKRIPSI



**ANALISIS KEAMANAN *WEBSITE* TERHADAP SERANGAN *PACKET SNIFFING* DI JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
FAKULTAS TEKNIK UNIVERSITAS NEGERI MAKASSAR**

***WEBSITE SECURITY ANALYSIS OF INTERNET PACKET SNIFFING
ATTACKS IN INFORMATICS AND COMPUTER ENGINEERING
DEPARTMENT FACULTY OF ENGINEERING STATE UNIVERSITY OF
MAKASSAR***

SUCI RAHMAHDANY

1929140013

**PROGRAM STUDI TEKNIK KOMPUTER
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
FAKULTAS TEKNIK
UNIVERSITAS NEGERI MAKASSAR**

2023



SKRIPSI

**ANALISIS KEAMANAN *WEBSITE* TERHADAP SERANGAN *PACKET SNIFFING* DI JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
FAKULTAS TEKNIK UNIVERSITAS NEGERI MAKASSAR**

*Diajukan kepada Program Studi Teknik Komputer Fakultas Teknik untuk
Memenuhi Salah Satu Syarat Memperoleh Gelar Sarjana*

SUCI RAHMAHDANY

1929140013

**PROGRAM STUDI TEKNIK KOMPUTER
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
FAKULTAS TEKNIK
UNIVERSITAS NEGERI MAKASSAR**

2023

LEMBAR PENGESAHAN SKRIPSI



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR (UNM)
FAKULTAS TEKNIK
Alamat: Jalan Daeng Tata Raya Parangtambung Makassar
Telp (0411) 865677 – Fax. (0411) 861377
Laman: ft.unm.ac.id

PENGESAHAN SKRIPSI

Skripsi ini diajukan oleh:

Nama : Suci Rahmahdany
NIM : 1929140013
Judul : Analisis Keamanan Website Terhadap Serangan Packet Sniffing di
Jurusan Teknik Informatika dan Komputer Universitas Negeri
Makassar
Nomor SK : 4202/UN36.2/PP/OL/2023

telah dipertahankan di hadapan Dewan Penguji pada hari Kamis, tanggal 19 Oktober 2023 dan dinyatakan dapat diterima sebagai bagian persyaratan memperoleh gelar **Sarjana Komputer** pada Program Studi SI Teknik Komputer, Jurusan Teknik Informatika dan Komputer, Fakultas Teknik, Universitas Negeri Makassar.

Disahkan oleh:
Dekan Fakultas Teknik
Universitas Negeri Makassar

Prof. Dr. Ir. Muhammad Yahya, M.Kes., M.Eng. IPU., ASEAN Eng.
196306231991031002

Panitia Ujian :

Ketua Penguji : Prof. Dr. Ir. Muhammad Yahya, M.Kes., M.Eng. IPU.,
ASEAN Eng.

Sekretaris
Penguji : Dr. Ir. Mustari S. Lamada, S.Pd., M.T.

Pembimbing I : Dr. Ir. Mustari S. Lamada, S.Pd., M.T.

Pembimbing II : Prof. Dr. Hendra Jaya, S.Pd., M.T.

Penguji I : Dr. Muliadi, S.Pd., M.T.

Penguji II : Alifya Nfh, S.Pd., M.Pd.

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini:

Nama : Suci Rahmahdany
NIM : 1929140013
Program Studi : Teknik Komputer
Judul : Analisis Keamanan Website Terhadap Serangan Packet Sniffing di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar

Dengan ini menyatakan bahwa skripsi ini adalah hasil karya yang bersumber ide saya sendiri dan bukan mengambil alih tulisan atau pikiran orang lain, kecuali yang saya nyatakan dalam kutipan. Selain itu, tidak ada bagian dari skripsi yang telah saya atau orang lain gunakan sebelumnya untuk memperoleh gelar akademik.

Jika kemudian hari pernyataan diatas terbukti dan tidak benar, maka saya bersedia diberikan sanksi yang telah ditetapkan oleh Fakultas Teknik Universitas Negeri Makassar berdasarkan peraturan yang telah ditetapkan

Makassar, 19 Oktober 2023

Yang membuat pernyataan



SUCI RAHMAHDANY

HALAMAN PERSEMBAHAN

الرَّحِيمِ الرَّحْمَنِ اللَّهُ بِسْمِ

Karya ini saya persembahkan untuk:

Diri Saya Sendiri

Yang telah melewati perjalanan yang panjang dan penuh tantangan untuk menyelesaikan skripsi ini. Selama perjalanan itu, ada banyak saat-saat sulit dan keraguan, tetapi saya terus berjuang menikmati proses demi proses. Saya memutuskan untuk percaya pada kemampuan diri sendiri, dan ini adalah bukti bahwa apapun bisa dicapai jika kita benar-benar berusaha.

Almarhum Ayahanda, Ibunda dan Saudara(i) Tersayang

Terima kasih atas segala pengorbanan dan doa yang selalu kalian panjatkan setiap hari.

Terima kasih atas nasihat bijak yang selalu memberikan arahan dan dukungan dalam setiap pilihan yang saya buat

Terima kasih atas dukungan moral, semangat, dan kebahagiaan yang kalian berikan.

Orang-Orang Yang Tak Sedarah, Tapi Selalu Ada

Terima kasih tidak pernah membuat saya merasa sendirian.

Kebersamaan kita adalah bukti bahwa keluarga tidak selalu harus diukur dengan darah, tetapi dengan cinta dan kesetiaan.

Surgaki.

Prodi Teknik Komputer, Universitas Negeri Makassar

Terima kasih yang tak terhingga kepada almamater tercinta yang merupakan kebanggaan dari program studi Teknik Komputer, Jurusan Teknik Informatika dan Komputer, Fakultas Teknik, di Universitas Negeri Makassar.

MOTTO

“Ketahuilah bahwa kehidupanmu mengikuti jalan pikiranmu, jadi jika hal itu berupa pikiran yang bermanfaat bagimu dalam urusan agama atau dunia, maka kehidupanmu baik dan Bahagia, jika tidak maka perkaranya yang sebaliknya.”

-Asy-Syaikh Abdurrahman AS-Sa'dy rahimanullah

“Sebaik-baiknya manusia, adalah manusia yang bermanfaat untuk diri sendiri dan orang lain. Dalam hal ini teladan terbaik yaitu Rasulullah SAW. dan para Sahabat.”

– Habib Ja'Far Al Jufri

“Bersyukur itu bukan karena semuanya baik-baik saja, tapi karena kita percaya selalu ada sisi baik dibalik sesuatu yang kita anggap tidak baik.”

-Unknown

“Happiness and confidence are the prettiest things you can wear”

-Taylor Swift

"Pendidikan bukanlah satu-satunya jalan menuju sukses. Tapi, jika Anda tahu pendidikan adalah jalan Anda, maka Anda harus mengikutinya."

- Reply 1997

"Kadang-kadang, hidup adalah tentang mengejar hal-hal kecil yang membuat kita bahagia."

- Weightlifting Fairy Kim Bok Joo

ABSTRAK

Suci Rahmahdany, 2023. Analisis Keamanan *Website* Terhadap Serangan *Packet Sniffing* Di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar. Program Studi Teknik Komputer, Jurusan Teknik Informatika dan Komputer, Fakultas Teknik. Universitas Negeri Makassar (dibimbing oleh Mustari S. Lamada dan Hendra Jaya).

Di Jurusan Teknik Informatika dan Komputer memiliki beberapa *website* yang dibuat khusus untuk mahasiswa JTik dengan manfaatnya masing-masing seperti SIMPEL, SIM-TA, IDS (*Integrated Data System*), Sigmatik, dan SIPI. Penelitian ini bertujuan untuk mengetahui tingkat kerentanan terhadap serangan *packet sniffing* pada *website* yang berada di Jurusan Teknik Informatika dan Komputer Universitas Negeri Makassar. Metode penelitian ini menggunakan pendekatan kualitatif dengan melakukan uji coba serangan *sniffing* terhadap beberapa *User* pada *website* yang dituju. Hasil analisis uji coba serangan *packet sniffing* menunjukkan adanya potensi kerentanan terhadap upaya pencurian data melalui metode serangan *sniffing* pada jaringan nirkabel di beberapa *website* yang diteliti. Dalam konteks ini, *website* SIMPEL, IDS, dan SIMTA dapat dianggap sebagai *website* yang relatif aman. Dalam uji coba serangan terhadap beberapa *hotspot*, *User*, dan perangkat, tidak ada informasi yang dapat ditemukan selain konfirmasi bahwa *website-website* tersebut telah dienkripsi menggunakan protokol keamanan yang sesuai. Sebaliknya, *website* Sigmatik dan SIPI menunjukkan tingkat kerentanan yang lebih tinggi. Data sensitif seperti *Username* dan *password* yang digunakan selama proses *login* dapat terlihat dalam uji coba serangan. Hal ini terjadi karena *website* Sigmatik dan SIPI masih menggunakan protokol HTTP yang tidak aman, sedangkan *website* SIM-TA, SIMPEL, dan lainnya telah beralih ke protokol TLS/SSL atau HTTPS yang lebih aman. Hasil identifikasi dari penelitian ini yaitu mendapatkan informasi berupa jenis koneksi dan protokol yang digunakan, jenis pesan seperti POST dan GET, jenis *port*, *host* atau server, jenis *browser* yang digunakan, Bahasa, jenis server yang digunakan, serta data sensitif *username* dan *password*. Rekomendasi penting yang dihasilkan dari penelitian ini adalah perlunya perancangan sistem pemantauan dan deteksi yang dapat dengan cepat mengenali potensi serangan *packet sniffing*. Penelitian ini diharapkan dapat menjadi dasar untuk meningkatkan kesadaran dan upaya keamanan *website* di lingkungan akademik dan dapat diterapkan pada konteks yang lebih luas di dunia digital.

Kata Kunci: Keamanan Website, Serangan *Packet Sniffing*, Analisis Keamanan

ABSTRACT

Suci Rahmahdany, 2023. Website Security Analysis of Packet Sniffing Attacks in the Department of Information and Computer Engineering, Faculty of Engineering, Makassar State University. Computer Engineering Study Program, Department of Informatics and Computer Engineering, Faculty of Engineering. Makassar State University (guided by Mustari S. Lamada and Hendra Jaya).

The Department of Informatics and Computer Engineering has several websites specially made for JTIK students with their respective benefits, such as SIMPEL, SIM-TA, IDS (Integrated Data System), Sigmatik, and SIPI. This research aims to determine the level of vulnerability to packet sniffing attacks on websites at the Department of Information and Computer Engineering, Makassar State University. This research method uses a qualitative approach by testing sniffing attacks on several *Users* on the targeted website. The results of the analysis of packet sniffing attack trials show that there is a potential vulnerability to data theft attempts through sniffing attack methods on wireless networks on several websites studied. In this context, the SIMPEL, IDS, and SIMTA websites can be considered relatively safe websites. In test attacks against multiple hotspots, *Users*, and devices, no information could be found other than confirmation that the website was encrypted using appropriate security protocols. In reverse, the Sigmatik and SIPI websites showed a higher level of vulnerability. Sensitive data such as *Username*s and passwords used during the login process can be visible in test attacks. It happens because the Sigmatik and SIPI websites still use the insecure HTTP protocol, while the SIM-TA, SIMPEL and other websites have switched to the more secure TLS/SSL or HTTPS protocol. The identification results of this research are obtaining information in the form of the type of connection and protocol used, message types such as POST and GET, type of port, host or server, type of browser used, language, type of server used, as well as sensitive user name and password data. An important recommendation resulting from this research is the need to design a monitoring and detection system that can quickly recognize potential packet sniffing attacks. It is hoped that this research can become the basis for increasing awareness and efforts on website security in the academic environment and can be applied to a broader context in the digital world.

Keywords: *Website Security, Packet Sniffing Attacks, Security Analysis*

KATA PENGANTAR

Puji syukur kehadiran Allah SWT yang telah melimpahkan rahmat, hidayah, serta karunia-Nya kepada penulis sehingga dapat menyelesaikan penelitian ini dengan judul "**Analisis Keamanan Website Terhadap Serangan *Packet Sniffing* di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar**". Penulisan skripsi ini merupakan bagian dari perjalanan akademik dan salah satu syarat untuk memperoleh gelar Sarjana Komputer dengan konsentrasi Jaringan dari Program Studi Teknik Komputer pada Fakultas Teknik Universitas Negeri Makassar.

Penulis berterima kasih kepada Ibunda penulis yang tersayang Sri Wanti Hasnia dan ke-9 saudara penulis yang telah mendoakan dan memberikan dukungan selama ini. Penyusunan skripsi ini tidak akan terwujud tanpa dukungan, bimbingan, dan dorongan dari berbagai pihak yang dengan tulus ikhlas telah membantu penulis. Oleh karena itu, penulis ingin mengucapkan terima kasih yang tulus kepada:

1. Prof. Dr. H. Husain Syam, M.TP., IPU., ANSEAN, Eng., sebagai Rektor Universitas Negeri Makassar;
2. Prof. Ir. H. Muhammad Yahya, M. Kes., M.Eng., IPU., sebagai Dekan Universitas Negeri Makassar;
3. Dr. Mustari S. Lamada, M.T., sebagai Ketua Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar;
4. Dr. Sanatang, S.Pd., M.T., sebagai Sekertaris Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar;
5. Dr. Satria Gunawan Zain, S.Pd., M.T., sebagai Ketua Program Studi Teknik Komputer, Fakultas Teknik Universitas Negeri Makassar;
6. Bapak Dr. Mustari S. Lamada, M.T., sebagai Dosen Pembimbing Akademik sekaligus Dosen Pembimbing I yang telah memberikan arahan dan bimbingan kepada penulis dalam menjalani proses perkuliahan dan proses penulisan hingga dapat diselesaikan dengan baik, serta ilmu yang berharga yang telah diberikan selama proses penelitian ini;
7. Bapak Prof. Dr. Hendra Jaya, S.Pd., M.T., sebagai Dosen Pembimbing II yang telah menyisihkan waktunya untuk memberikan bimbingan kepada penulis selama proses penelitian sehingga penulisan skripsi ini selesai sesuai tenggat waktu yang ditentukan;

8. Bapak Dr. Muliadi, S.Pd., M.T., sebagai Penanggap 1;
9. Ibu Alifya Nfh, S.Pd., M.Pd., sebagai Penanggap 2;
10. Bapak/Ibu dosen pengajar serta staff Jurusan Teknik Informatika dan Komputer, Universitas Negeri Makassar yang telah memberikan ilmunya kepada penulis selama perkuliahan;
11. Terima kasih kepada keluarga tercinta, Kakak penulis Wawan Hermanto dan istrinya Murniatiningsih yang telah menjadi orang tua kedua yang selalu memberikan dukungan finansial, moral, dan mendidik ke nilai-nilai yang baik kepada penulis dalam setiap langkah perjalanan akademik;
12. Terima kasih kepada Elva Amalia, dan Andi Nurul Izzah yang banyak mengajarkan penulis banyak hal dan memberikan semangat motivasi, nasihat serta dukungan kepada penulis;
13. Irmayanti Syarif, Nurul Faradillah, dan Miftahul Jannah sahabat dari bangku SMA yang selalu mengirimkan doa terbaiknya.
14. Teman-teman dilembaga tercinta UKM KSR PMI UNM, khususnya Faizal Cahya Alim, Tiara Putri Amelia, Winny Wirasti Mala', Fitria Suci, dan seluruh Angkatan 34.
15. Teman-teman seangkatan lainnya di Prodi Teknik Komputer yang telah berbagi pengetahuan dan pengalaman selama masa perkuliahan.
16. Serta semua pihak yang telah memberikan dukungan kepada penulis yang tidak dapat disebutkan satu per satu.

Penulis menyadari bahwa penelitian ini jauh dari kata sempurna, dan masih banyak ruang untuk perbaikan di masa mendatang. Semoga hasil penelitian ini dapat memberikan kontribusi kecil dalam pemahaman lebih lanjut tentang keamanan *website* dan menjadi landasan untuk penelitian-penelitian selanjutnya.

Makassar, 27 September 2023

Penulis,

Suci Rahmahdany

DAFTAR ISI

HALAMAN JUDUL	ii
LEMBAR PENGESAHAN SKRIPSI	iii
HALAMAN PERSEMBAHAN	v
MOTTO	vi
ABSTRAK.....	vii
ABSTRACT	viii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	xi
DAFTAR GAMBAR.....	xiii
DAFTAR TABEL	xiv
DAFTAR LAMPIRAN	xv
BAB I PENDAHULUAN.....	1
A. Latar Belakang.....	1
B. Rumusan Masalah.....	4
C. Tujuan Penelitian	5
D. Manfaat Penelitian	5
BAB II TINJAUAN PUSTAKA	7
A. Kajian Teori.....	7
1. Internet	7
2. Jaringan Komputer.....	8
3. <i>Website</i>	11
4. <i>Wireless Fidelity</i> (Wi-Fi)	15
5. <i>Keamanan Website</i>	17
6. <i>Cybercrime</i>	20
7. <i>Packet sniffing</i>	22
8. <i>Wireshark</i>	25
9. <i>Etercap</i>	27
B. Kajian Penelitian yang relevan.....	29
C. Kerangka Pikir.....	34

BAB III METODE PENELITIAN	36
A. Jenis Penelitian	36
B. Waktu dan Tempat Penelitian	36
C. Teknik Pengumpulan Data	36
D. Teknik Analisis Data	37
E. Alat dan Bahan	37
F. Prosedur Penelitian	38
G. Rancangan Penelitian.....	40
BAB IV HASIL DAN PEMBAHASAN.....	45
A. Hasil Penelitian.....	45
B. Pembahasan	73
BAB V PENUTUP	79
A. Kesimpulan.....	79
B. Saran	80
DAFTAR PUSTAKA.....	81
LAMPIRAN	83

DAFTAR GAMBAR

Gambar 2. 1 Komponen Jaringan Komputer.....	10
Gambar 2. 2 Alur Protokol HTTP	12
Gambar 2. 3 Perbedaan Protokol HTTP dan HTTPS	13
Gambar 2. 4 <i>Wireless Fidelity</i>	16
Gambar 2. 5 Keamanan Jaringan Internet Menggunakan <i>Firewall</i>	18
Gambar 2. 6 Cara Kerja SSL.....	19
Gambar 2. 7 <i>Packet Sniffing</i>	23
Gambar 2. 8 <i>Wireshark Interfaces</i>	27
Gambar 2. 9 Kerangka Pikir	34
Gambar 3. 1 Diagram Alir Penelitian	39
Gambar 3. 2 Skema Penelitian	41
Gambar 4. 1 Koneksi Jaringan Nirkabel	46
Gambar 4. 2 Tampilan <i>Interfaces Ettercap</i>	46
Gambar 4. 3 Memulai <i>sniffing</i>	47
Gambar 4. 4 <i>Scanning Host</i> yang terkoneksi	48
Gambar 4. 5 Daftar <i>host</i>	48
Gambar 4. 6 target 1 <i>gateway</i>	49
Gambar 4. 7 Menentukan target 2	50
Gambar 4. 8 <i>ARP Poisoning</i>	50
Gambar 4. 9 Proses Transmisi Data.....	51
Gambar 4. 10 Tampilan awal <i>Wireshark</i>	52
Gambar 4. 11 Proses <i>Scanning</i> Jaringan.....	52
Gambar 4. 12 Paket Data Target	53
Gambar 4. 13 Proses <i>Login</i> pada <i>Website</i>	54
Gambar 4. 14 <i>Stop Capture</i>	54
Gambar 4. 15 <i>Capture Packet Sniffing</i> pada <i>Wireshark</i>	59
Gambar 4. 16 IP Address <i>Website</i> Sigmatik	60
Gambar 4. 17 Paket data dari <i>website</i> Sigmatik	61
Gambar 4. 18 Rincian <i>Packet TCP</i>	62
Gambar 4. 19 <i>Filtering</i> Protokol HTTP.....	63
Gambar 4. 20 Paket data <i>website</i> SIMPEL yang Terekam	64
Gambar 4. 21 Rincian <i>packet data TCP</i>	65
Gambar 4. 22 Isi <i>Packet Follow HTTP Stream</i>	67
Gambar 4. 23 Isi paket data <i>Follow TLS Stream</i> dan <i>TCP Stream</i>	71
Gambar 4. 24 Proses Komunikasi Data <i>Client</i> dan <i>Server</i>	72
Gambar 4. 25 Proses Komunikasi Data <i>Client</i> dan <i>Server</i>	73
Gambar 4. 26 Proses Komunikasi Data <i>Website</i> Sigmatik dan SIPI.....	74
Gambar 4. 27 Proses Komunikasi Data Protokol HTTPS Pada <i>Website</i> SIM-TA	76

DAFTAR TABEL

Tabel 2. 1 Macam-macam <i>port</i>	8
Tabel 2. 2 Kajian Pustaka.....	33
Tabel 3. 1 Hasil Observasi	42
Tabel 3. 2 Hasil Pengujian	44
Tabel 4. 1 Hasil Penelitian Menggunakan <i>Hotspot</i> Broadband_UNM	56
Tabel 4. 2 Hasil Penelitian Menggunakan <i>Hotspot</i> Pribadi	57
Tabel 4. 3 IP Address Website JTIK	60
Tabel 4. 4 Analisis Rincian <i>packet</i> data.....	62
Tabel 4. 5 Analisis Rincian <i>Packet Data</i> HTTPS	65
Tabel 4. 6 Hasil Identifikasi paket data Website Sigmatik.....	69
Tabel 4. 7 Hasil Identifikasi paket data Website SIPI	70

DAFTAR LAMPIRAN

Lampiran 1. 1 Hasil Uji Coba Serangan <i>Packet Sniffing</i>	84
Lampiran 1. 2 Persuratan	95

BAB I

PENDAHULUAN

A. Latar Belakang

Menurut data yang dikeluarkan oleh Kementrian Komunikasi dan Informatika (Kemenkominfo), jumlah pengguna internet di Indonesia saat ini 63 juta orang dimana 95% dari mereka memanfaatkan internet untuk mengakses platform sosial. Berbeda dari saat pertama kali hadir, internet saat ini telah banyak dimanfaatkan oleh berbagai entitas, terutama yang beroperasi dalam ranah teknologi. Didalam ranah internet, salah satu fitur yang umumnya dipakai adalah situs web. Pada awalnya situs web hanya terdiri dari situs statis, namun kini banyak yang berubah menjadi lebih dinamis dan interaktif dalam penggunaannya dalam sistem informasi telekomunikasi. Internet atau web adalah jaringan komputer yang saling terhubung diseluruh dunia. Kehadiran web menjadi sangat penting ditengah era globalisasi ini (Lamada, 2020). Pemanfaatan web saat ini sangat membantu dalam berbagai bidang. Terutama dalam dunia pendidikan, web memudahkan pelajar untuk mendapatkan segala informasi dengan mudah.

Universitas Negeri Makassar adalah salah satu kampus yang memanfaatkan keberadaan *website* sebagai sumber data dan informasi untuk memudahkan mengakses informasi dan menyimpan semua data baik itu data pribadi, data mahasiswa, maupun data kampus yang bersifat tertutup. *Website* ini digunakan oleh mahasiswa, dosen, dan staff dalam konteks aktivitas akademik serta sebagai sarana untuk mengakses informasi terbaru mengenai Universitas Negeri Makassar.

Di Jurusan Teknik Informatika dan Komputer memiliki beberapa *website* yang dibuat khusus untuk mahasiswa JTIC dengan manfaatnya masing-masing seperti SIMPEL, SIM-TA, IDS (*Integrated Data System*), Sigmatik, dan SIPI. Dengan adanya *website* ini dapat memudahkan bagian administrasi dalam melakukan pemrosesan data dimana admin tidak diperlukan lagi interaksi tatap muka secara langsung, serta memudahkan untuk mengolah data-data seperti pengumpulan berkas, pengajuan judul, monitoring tugas akhir, monitoring praktek industri dan sumber informasi lainnya. Untuk mengakses data pada *website-website* tersebut tentunya diperlukan *login* menggunakan akun masing-masing mahasiswa yang telah terdaftar.

Keberadaan *website* ini sangat berguna bagi beberapa pihak. Namun, Monirruzman pada penelitiannya mengatakan bahwa tidak ada *website* yang dapat terhindar dari resiko kerentanan terhadap serangan siber. Salah satu serangan siber yang banyak terjadi didunia maya dan jarang diketahui oleh orang awam yaitu serangan *packet sniffing*. *Packet sniffing* merupakan salah satu jenis serangan yang dapat merekam informasi dari paket data yang melewati jaringan dimana pelaku yang melakukan tindakan tersebut dapat mengambil informasi seperti nama pengguna (*Username*), kata sandi, dan data penting lainnya dalam bentuk teks yang mengalir melalui jaringan tanpa sepengetahuan dan izin dari pengguna. Pelaku dapat mengubah data atau melakukan segala hal dengan data yang telah didapatkan secara ilegal, sehingga hal tersebut dapat merugikan dan membahayakan privasi para pengguna yang beraktivitas didunia maya (Rizkiyani, 2020).

Adapun pada penelitian sebelumnya, Aji Supriyanto melakukan analisis kerentanan dalam jaringan nirkabel dimana sistem jaringan ini memiliki masalah terkait keamanan spesifik yang mempengaruhi beberapa aspek keamanan. Salah satu aspek sistem keamanan *wireless* yang dibahas ialah penyadapan pada jalur komunikasi yang dapat dijalankan dengan simpel karena tidak membutuhkan kabel untuk menghubungkan komputer tersebut. Apabila metode keamanannya tidak memanfaatkan pengaman dan verifikasi, dan tidak ada upaya pencegahan, jaringan akan mudah disadap. Oleh karena itu, diperlukan langkah keamanan yang lebih spesifik pada perangkat komunikasi yang digunakan. Sementara itu, penelitian oleh Syaifuddin pada tahun (2017) melakukan percobaan komunikasi antara PC1 dan PC2 yang sedang bertukar data, dengan PC3 sebagai *cyber crime* yang dapat merusak celah keamanan pada jaringan dengan mengelabui PC target menjadi salah satu *host* yang sah yang tujuannya untuk melakukan *sniffing active*. Dengan hasil PC3 yang berhasil mengelabui PC1 dan PC2 yang sedang berkomunikasi atau bertukar informasi, maka paket komunikasi atau informasi tersebut dapat dialihkan. Kemudian penelitian selanjutnya dilakukan rancangan untuk sebuah sistem keamanan jaringan di sebuah perusahaan yang mempunyai fasilitas jaringan nirkabel (Wi-Fi) dengan melakukan konfigurasi dan implementasi menggunakan aplikasi dan beberapa *tools* dengan memanfaatkan *information detection system* (ids). Uji coba yang dilakukan berawal dari *User* yang akan terkoneksi dengan *access point* yang sudah ada, setelah itu PC yang melakukan serangan memulai serangan *packet sniffing* terhadap *access point*. Hasil penelitian menunjukkan bahwa sistem keamanan jaringan pada perusahaan tersebut belum maksimal atau

keamanan terancam karena segala aktivitas pengguna dapat dengan mudah direkam dan menjadi sasaran pencurian data. (Kurniawan, 2020).

Dengan dasar isu yang telah disebutkan, penulis merasa tertarik untuk menjalankan analisis keamanan *website* yang digunakan oleh mahasiswa, staff, serta dosen di Jurusan Teknik Informatika Fakultas Teknik Universitas Negeri Makassar. Uji coba keamanan ini dilakukan dengan tujuan untuk mengetahui tingkat kerentanan sistem keamanan *website* terhadap serangan *packet sniffing* dengan menggunakan beberapa aplikasi penganalisa jaringan seperti aplikasi *Wireshark* dan *Ettercap*. Sehingga, hasil yang diharapkan penulis yaitu dapat menggunakan *website* dengan keamanan privasi yang terjaga dari risiko serangan pemantauau paket data atau *packet sniffing* yang dapat mengancam keamanan harus data para pengguna *website* yang terhubung di jaringan nirkabel yang sama.

B. Rumusan Masalah

Berdasarkan konteks latar belakang yang telah dijelaskan, maka permasalahan yang akan diteliti dapat dirumuskan sebagai berikut:

1. Bagaimana tingkat kerentanan terhadap serangan *packet sniffing* pada *website* di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar?
2. Bagaimana hasil identifikasi dari serangan *packet sniffing* pada *website* di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar?

C. Tujuan Penelitian

Penulis memiliki tujuan sebagai berikut dalam penelitian ini:

1. Untuk mengetahui tingkat kerentanan terhadap serangan *packet sniffing* pada *website* di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar.
2. Untuk mengetahui hasil identifikasi dari serangan *packet sniffing* pada *website* di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar.

D. Manfaat Penelitian

Manfaat dari penelitian ini mencakup:

1. Manfaat Teoritis
 - a. Diharapkan bahwa hasil penelitian ini akan memperkaya pemahaman dan pengetahuan mengenai topik yang berhubungan dengan keamanan *website* pada saat menggunakan *hotspot* yang umum digunakan.
 - b. Diharapkan bahwa hasil penelitian ini dapat digunakan sebagai referensi/acuan untuk penelitian yang akan datang.
2. Manfaat Praktis
 - a. Bagi pengelola jaringan, penelitian ini diharapkan dapat menjadi sebuah informasi terkait tingkat kerentanan keamanan jaringan serta *website* untuk selanjutnya ditindak lanjuti.

- b. Bagi *web developer*, diharapkan bahwa hasil penelitian ini dapat digunakan sebagai pertimbangan dan masukan dalam upaya meningkatkan keamanan *website* menjadi lebih baik.
- c. Bagi *user* (pengguna), diharapkan bahwa hasil penelitian ini dapat meningkatkan pemahaman tentang betapa pentingnya keamanan *website* dalam menggunakan jaringan yang bersifat publik atau umum terutama bagi pengguna terhadap potensi risiko *website* yang tidak aman.

BAB II

TINJAUAN PUSTAKA

A. Kajian Teori

1. Internet

Interconnected-Networking, yang sering disebut sebagai internet, adalah sistem komunikasi yang memiliki kemampuan untuk menghubungkan jaringan komputer dari berbagai negara diseluruh dunia dimana memungkinkan individu untuk berkomunikasi secara global, serta dapat bertukar data, dan informasi melalui internet menggunakan aturan protokol standar yang disebut *Transmission Control Protocol* dan *Internet Protocol*, yang sering disingkat sebagai TCP/IP (Rodhin, 2012).

TCP/IP merupakan standar komunikasi data dalam jaringan yang memungkinkan perangkat-perangkat berbagi informasi diseluruh internet. TCP dan IP ini memiliki fungsi masing-masing, dimana TCP (*Transmission Control Protocol*) berfungsi untuk memastikan kelancaran semua koneksi diseluruh sistem, sedangkan IP (*Internet Protocol*) bertanggung jawab atas transmisi data dari satu komputer ke komputer lainnya (M. Syaifuddin, 2017).

Port merupakan akses yang dimanfaatkan oleh sebuah *node* IP untuk mengirim dan menerima data. Rentang *port* adalah 0-65536. *Port* 0-1024 disebut *port* terkenal (*well known port*) yang telah diatur berdasarkan standar. Beberapa model *port* TCP dan UDP yang terkenal ditampilkan pada Tabel 2.1 Macam-macam *port* berikut:

Tabel 2. 1 Macam-macam *port*

TCP		UDP	
Nomor <i>Port</i>	Aplikasi	Nomor <i>Port</i>	Aplikasi
20/21	FTP	15	Nestat
23	Telnet	53	DNS
25	SMTP	67/68	DHCP
80	HTTP	137	Netbios
110	POP3	161	SMP

2. Jaringan Komputer

Melwin Syafrizal pada bukunya yang berjudul “*Pengantar Jaringan Komputer*” tahun 2005 mengemukakan jaringan komputer pada sekelompok komputer dan perangkat lain yang saling terhubung satu sama lain menggunakan berbagai jenis media transmisi, seperti kabel atau tanpa nirkabel (*wireless*). Sumber daya yang beragam, seperti printer, CD-ROM, pertukaran file, dan komunikasi elektronik, dapat saling terkoneksi. Hal ini memungkinkan akses ke aplikasi di server yang jauh, mencetak, mengirim file, dan sebagainya, semuanya merupakan elemen dari jaringan komputer.

Umumnya, klasifikasi jaringan komputer biasanya terbagi menjadi tiga kategori, yaitu jaringan komputer berdasarkan pola pengoperasiannya, kemudian berdasarkan jangkauan, dan berdasarkan media transmisinya.

a. Berdasarkan Pola pengoperasiannya

Jaringan komputer memiliki tiga peranan penting dalam pengoperasiannya yang dapat dijalankan oleh komputer yaitu sebagai *client*, sebagai *peer*, dan sebagai *server*. Berdasarkan hal tersebut, jaringan komputer ini terdiri menjadi dua macam yakni:

- 1) Jaringan *client-server*, dimana peran klien disini hanya sebatas sebagai pengguna tanpa memberikan sumber daya jaringan untuk penggunaan bersama. Artinya, adanya *server* dalam jaringan dapat memberikan sistem pengamanan dan pengaturan untuk mengelola jaringan tersebut. *Client* dapat dikatakan sebagai komputer *front-end* dimana ia bertugas untuk mengajukan permintaan untuk layanan seperti menyimpan data, juga mencetak pada *printer*. Sementara itu, *server* dikatakan sebagai komputer *back-end* bertugas untuk mengarahkan permintaan tersebut ke destinasi yang tepat.
- 2) Jaringan *peer-to-peer*, adalah model dimana setiap PC dapat berbagi sumber daya PC lain atau menyediakan sumber daya untuk digunakan PC lain. Artinya, dapat bertindak sebagai *client* atau *server* pada saat yang bersamaan.

b. Berdasarkan Jangkauan

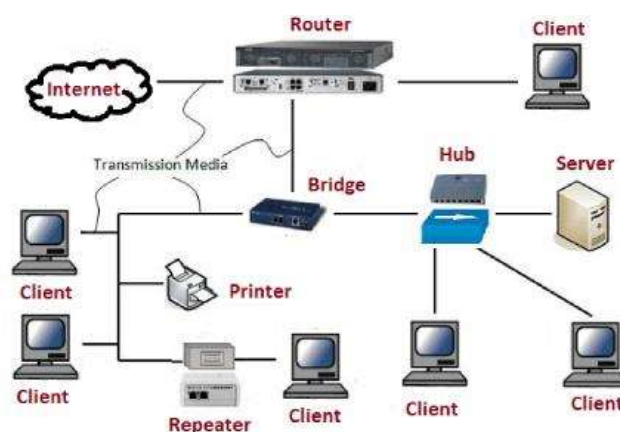
- 1) *Local Area Network* (LAN), merupakan jaringan yang memiliki cakupan terbatas, biasanya dibatasi oleh area fisik yang kecil seperti sebuah ruangan dalam gedung, perumahan, institusi pendidikan seperti sekolah atau kampus yang jarak jangkauannya kurang dari 1 km. LAN biasanya digunakan di kantor perusahaan dan pabrik untuk menghubungkan komputer pribadi dan *workstation* untuk berbagi sumber daya seperti printer, *scan*, dan melakukan pertukaran informasi.
- 2) *Metropolitan Area Network* (MAN) adalah jaringan komputer yang menggabungkan beberapa LAN menjadi satu kesatuan. Seperti

menghubungkan berbagai kampus, kantor, instansi, dan sebagainya. Jangkauan jaringan MAN lebih luas dibandingkan jaringan LAN.

- 3) *Wide Area Network* (WAN) sering memanfaatkan media *wireless*, satelit, atau serat optik dalam implementasinya. Hal ini untuk mencakup wilayah yang lebih besar karena WAN mulai menjangkau suatu wilayah atau antar kota bahkan dapat mencakup antarnegara.

c. Berdasarkan Media Transmisinya

- 1) Jaringan Kabel atau *Wire Network* merupakan jenis jaringan komputer yang memanfaatkan kabel sebagai medium penghubung. Kabel ini berfungsi untuk mentransmisikan data dalam bentuk sinyal listrik antara komputer dalam jaringan, biasanya digunakan dalam LAN.
- 2) Jaringan Nirkabel (*Wireless*), adalah jaringan yang tidak menggunakan kabel sebagai media penghubung, melainkan memanfaatkan media lain sebagai penghubung diantaranya yaitu *Bluetooth*, *Wi-Fi*, dan *InfraRed*.



Gambar 2. 1 Komponen Jaringan Komputer
Sumber: (<https://mediaindonesia.com>, 2023)

3. *Website*

Website ialah sekumpulan laman internet terkait, dapat diakses melalui internet dan berada dibawah domain atau alamat web tertentu. Halaman-halaman web ini biasanya berisi teks, gambar, video, dan elemen multimedia lainnya yang ditampilkan menerapkan bahasa pemrograman web seperti HTML (*Hypertext Markup Language*), CSS (*Cascading Style Sheets*), dan JavaScript. *Website* dapat berupa situs web statis, dimana kontennya tidak berubah atau situs web yang bersifat dinamis, dimana kontennya dapat berubah secara otomatis sesuai dengan interaksi dari pengguna atau dari server yang menerima data (Rochmawati, 2019).

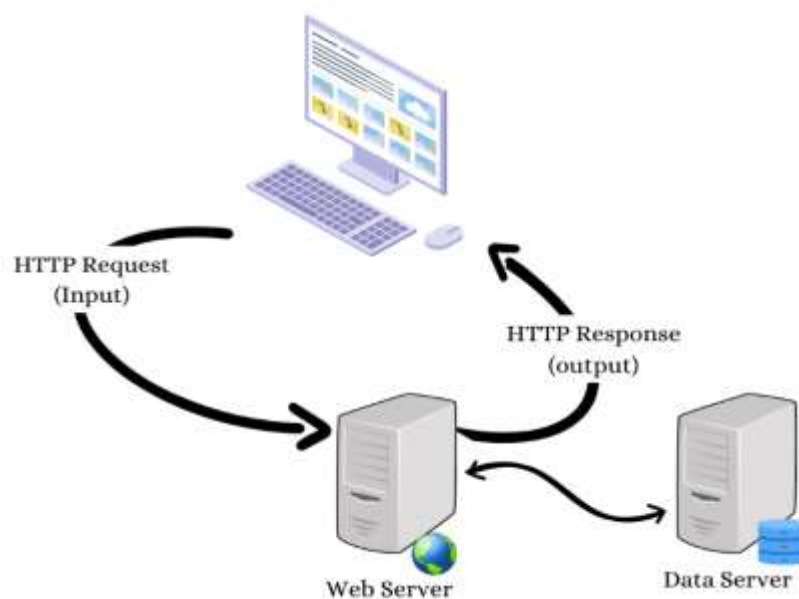
a. **Web Server**

Web server atau server web merupakan *software* yang dirancang untuk memuat, mengurus, dan menyampaikan isi situs web kepada pengguna melalui jaringan internet. Khususnya, server web memiliki tugas menampung permintaan dari *client* seperti *web browser*, dan aplikasi lain. Selanjutnya *web server* akan memproses permintaan tersebut, dan memberikan respon dari data yang diminta. Untuk menerima permintaan dari *web browser*, web server mempunyai beberapa protokol tersendiri. Berikut adalah beberapa protokol web server yang umum:

1) HTTP (*Hyper Text Transfer Protocol*)

HTTP merupakan *portokol* standar yang dipakai untuk mengatur komunikasi *client* dan *server web*. Oleh karena itu, protokol ini paling umum digunakan untuk mengakses situs web dan menyajikan halaman web kepada pengguna melalui internet. Namun, HTTP tidak menyediakan

lapisan keamanan untuk data yang ditransfer, dalam arti bahwa data dikirim dalam teks biasa (*plain text*). Hal ini membuat data yang dikirim melalui HTTP rentan terhadap pencurian atau penyadapan oleh pihak ketiga. Misalnya, ketika pengguna mengakses situs web melalui HTTP, informasi *login* seperti nama pengguna dan kata sandi tidak dienkripsi saat dikirim melalui jaringan. Disajikan Gambar 2.2 Alur Protokol HTTP berikut.

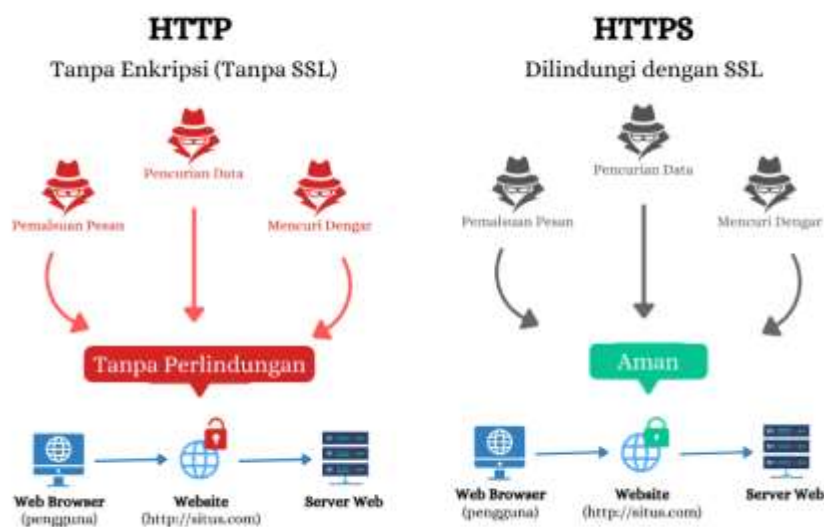


Gambar 2. 2 Alur Protokol HTTP

2) HTTPS (*Hypertext Transfer Protocol Secure*)

HTTPS adalah varian aman dari protokol HTTP yang menggunakan lapisan keamanan SSL/TLS (*Secure Sockets Layer/Transport Layer Security*) untuk mengenkripsi data yang ditransfer antara *client* dan *web server*. Protokol ini menyediakan keamanan tambahan untuk data yang dikirimkan antara *client* dan *server*, sehingga informasi sensitif menjadi terlindungi dari potensi peretasan atau penyadapan. Situs web yang menggunakan HTTPS

menampilkan ikon gembok atau kata “*Secure*” dibilah alamat *web browser*. Misalnya, ketika pengguna mengakses situs web menggunakan HTTPS, informasi *login* pengguna akan dienkripsi saat dikirimkan melalui jaringan, sehingga sulit bagi pihak ketiga untuk mencurinya (Jamaluddin & Suaeb, 2018).



Gambar 2. 3 Perbedaan Protokol HTTP dan HTTPS

b. Database Server

Database server ialah *software* juga sebagai *hardware* yang bertanggung jawab untuk memuat, mengurus, dan mengakses *database* secara efisien. *Database* adalah kumpulan data terstruktur yang disimpan secara sistematis dan terorganisir untuk pengolahan, penyimpanan, dan pengambilan data. Model *client-server* adalah representasi sistem yang memisahkan operasi sistem menjadi dua komponen, yakni server yang bertugas mengelola basis data dan klien yang menjalankan aplikasi. Server basis data memindahkan pengaksesan data dari klien ke server. Banyak klien dapat mengakses *database*

secara simultan, dan hanya satu sumber, yaitu database di server, yang dapat mengubah data yang diakses (Sutanto, 2015).

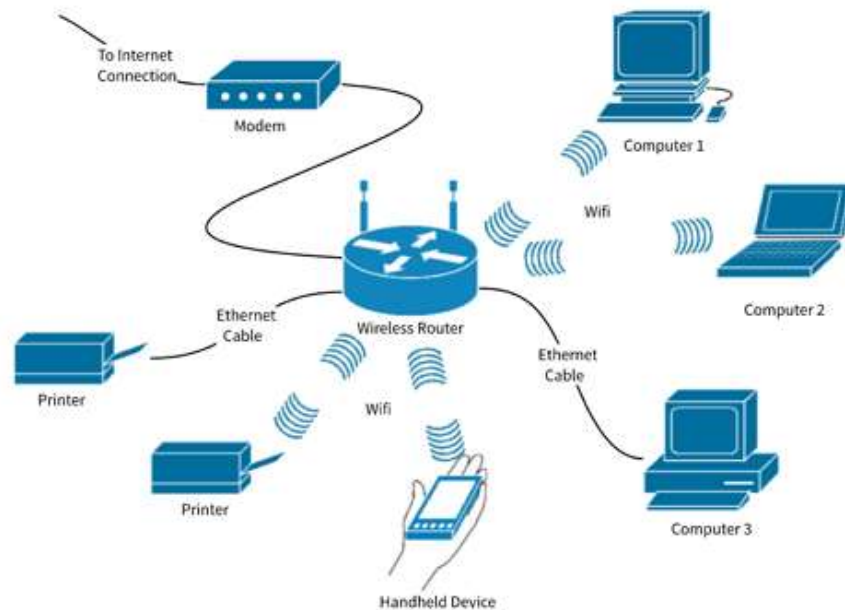
Website digunakan untuk berbagai tujuan, termasuk menyediakan informasi, berbagi konten, berkomunikasi, berinteraksi, dan melakukan transaksi online yang dapat diakses melalui perangkat seperti komputer, *smartphone*, tablet, dan perangkat lainnya yang terhubung ke internet. Penggunaan *website* memiliki berbagai manfaat bagi kampus dan institusi pendidikan. *Website* kampus menyediakan platform untuk menyebarkan informasi penting kepada mahasiswa, dosen, dan staff kampus. Informasi seperti jadwal kuliah, pengumuman, acara kampus, kegiatan ekstrakurikuler, dan informasi administratif dapat diakses dengan mudah melalui *website*. *Website* kampus dapat memudahkan pengelolaan akademik seperti penjadwalan kuliah, pengumuman nilai, dan transkrip akademik bagi mahasiswa serta dapat digunakan sebagai alat pemasaran untuk menarik calon mahasiswa dan menyampaikan informasi tentang keunggulan kampus dan program studi yang ditawarkan.

Beberapa *website* di Jurusan Teknik Informatika dan Komputer sangat bermanfaat bagi mahasiswa, seperti *website* SIMPEL yang digunakan mahasiswa untuk mengumpulkan judul untuk tugas akhir atau skripsi untuk diseleksi. Adapun *website* SIM-TA yang digunakan untuk memonitoring tugas akhir atau skripsi, mulai dari seminar proposal hingga ujian tutup selesai. IDS (*Intrgrated Data System*) berisi informasi pribadi seperti data pribadi, data orang tua, data akademik, riwayat Praktik Industri, riwayat pengajuan judul

hingga riwayat tugas akhir. *Website* Sistem Informasi Kegiatan Mahasiswa dan Dosen Jurusan Teknik Informatika dan Komputer yang disingkat menjadi Sigmatik berisi *event-event* yang diadakan oleh JTIK. Dengan mengoptimalkan manfaat *website*, kampus dapat memperkuat sistem informasi dan komunikasi, serta meningkatkan kualitas pelayanan akademik, dan memfasilitasi pengalaman belajar yang lebih efisien dan efektif bagi semua anggota kampus.

4. *Wireless Fidelity (Wi-Fi)*

Wireless mengembangkan salah satu aplikasi untuk komunikasi data yang disebut Wi-Fi. *Wireless Fidelity* atau yang sering disebut Wi-Fi ini adalah perangkat keras yang berperan dalam menghubungkan beberapa perangkat elektronik seperti PC, *printer*, perangkat seluler untuk saling bertukar data dan informasi melalui koneksi internet yang harus berada dalam satu titik akses (*hotspot*) dimana teknologi ini memanfaatkan frekuensi radio atau nirkabel. Sehingga, data-data digital yang dipindahkan melalui jaringan nirkabel akan diubah bentuk gelombang elektromagnetik (Wati & Apriansyah, 2019).



Gambar 2. 4 *Wireless Fidelity* (Wi-Fi)
 Sumber: (<https://www.nesabamedia.com>, 2022)

Seperti yang telah diketahui pada Gambar 2. 4 *Wireless Fidelity*, teknologi Wi-Fi tidak menggunakan kabel untuk koneksi akan tetapi menggunakan frekuensi radio. Dalam penggunaannya terdapat beberapa keuntungan bagi pengguna teknologi Wi-Fi diantaranya yaitu mobilitas. Mobilitas yaitu pengguna perangkat yang mendukung teknologi Wi-Fi ini tidak dibatasi oleh ruang dan jalur akses. Lebih tepatnya dapat sering berpindah-pindah tempat, namun tetap mempertahankan kecepatan koneksi yang stabil dalam jangkauan jaringan tertentu. Kemudian, keuntungannya yaitu hemat biaya dalam jangka panjang. Hal ini dibuktikan dengan biaya pemeliharaan jika menggunakan sambungan dengan kemampuan kabel untuk koneksi ke perangkat. Keuntungan selanjutnya, mudah terhubung di area publik dan sudah menjadi kebutuhan dalam masyarakat setempat (Abdillah, 2020).

Hotspot adalah wilayah yang ditutupi oleh satu *Access Point Wireless LAN* standar 802.11a/b/g, memungkinkan pengguna untuk terhubung ke *access point* tersebut secara bebas dan bergerak dengan perangkat *mobile*, seperti laptop, *smartphone* serta perangkat lainnya. Namun, *hotspot* yang akan dibahas pada penelitian ini berupa koneksi nirkabel ke jaringan internet menggunakan standar *wireless fidelity*.

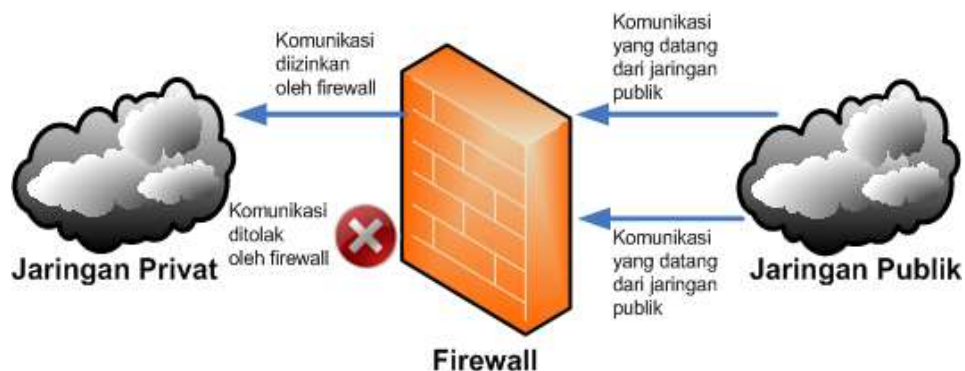
5. Keamanan Website

Perlindungan sistem harus diberlakukan untuk mencegah segala bentuk serangan atau upaya pemindaian oleh individu yang tidak memiliki otorisasi. Untuk itu definisi dari sistem keamanan *website* itu sendiri adalah suatu cara, praktik, serta tindakan yang diambil untuk memberikan proteksi pada situs web dari ancaman keamanan dan potensi serangan oleh pihak yang tidak berwenang. Mengamankan *website* sangat penting karena situs web yang rentan terhadap serangan dapat menghadapi risiko kehilangan data, peretasan, pencurian informasi, dan merusak reputasi.

Menurut Herdiana (2014), penggunaan teknologi Wi-Fi ini dapat dikategorikan menjadi tanpa pengaman (*Non-Secure*) dan menggunakan pengaman (*Share-Key/Secure*). Pada *Non-Secure* berarti Wi-Fi tidak menggunakan keamanan, dimana pengguna dapat mengakses jaringan tanpa ada bentuk keamanan yang diterapkan. Sedangkan, *Share Key* menggunakan kunci atau kata sandi sebagai alternatif keamanan jaringan Wi-Fi. Misalnya, jaringan yang menggunakan keamanan WEP. Pada *Wired Equivalent Privacy* (WEP) ini adalah standar keamanan nirkabel yang saat ini dapat dengan mudah diretas menggunakan

beberapa aplikasi yang tersedia secara bebas di internet. Kemudian, solusi untuk menggantikan WEP yaitu dengan keamanan WPA-PSK dan *Leap* yang perkembangannya kini juga sudah dapat diretas menggunakan metode *dictionary attack* secara *offline*. Hal ini dapat membuktikan bahwa tidak ada jaringan Wi-Fi yang dapat dipastikan sepenuhnya aman.

Teknologi Wi-Fi ini memanfaatkan frekuensi radio yang bersifat publik dan bebas untuk semua orang dengan pembatasan khusus. Batasan khusus disini artinya setiap jaringan Wi-Fi memiliki cakupan wilayah yang spesifik yang ditentukan oleh daya dan jenis antena yang digunakan. Ketika mengatur batasan cakupan area pada jaringan Wi-Fi tidaklah mudah. Seperti yang tampak pada Gambar 2.5 Keamanan Jaringan Internet menggunakan *Firewall*.

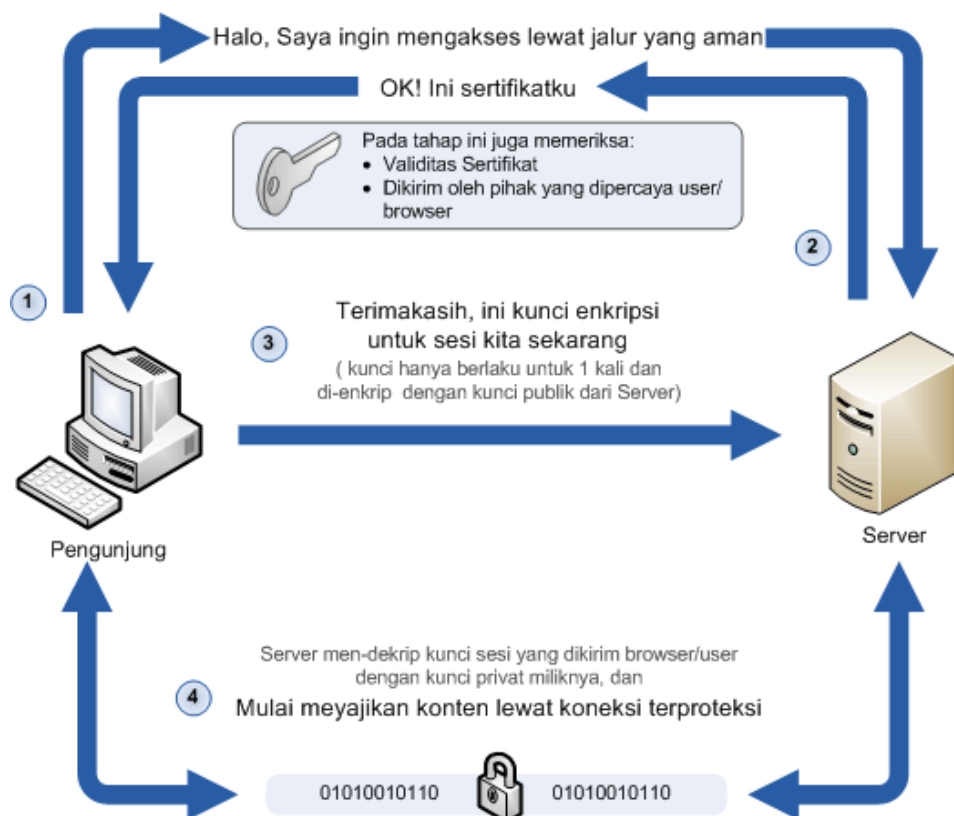


Gambar 2. 5 Keamanan Jaringan Internet Menggunakan *Firewall*

Sumber: (<https://aptika.kominfo.go.id>, 2017)

SSL (*Secure Socket Layer*) dan TLS (*Transport Layer Security*) merupakan dua protokol keamanan yang dipakai untuk mengenkripsi dan menjaga data yang dikirimkan antara perangkat dalam suatu jaringan, terutama saat berkomunikasi

melalui internet. Protokol ini menggunakan kriptografi untuk memberikan otentikasi dan privasi tertinggi saat berkomunikasi melalui internet. Umumnya, hanya server yang diautentikasi, kecuali sisi *client* diautentikasi dimana dalam hal ini server memiliki identitas unik. SSL bekerja diatas lapisan transport seperti TCP, dan dibawah lapisan aplikasi seperti HTTP, SMTP, atau FTP. Protokol SSL digunakan untuk melindungi integritas, kerahasiaan, dan keaslian data yang ditransfer antara server dan *client*. Sedangkan TLS adalah evolusi dari SSL dan diperkenalkan sebagai alternatif SSL yang lebih aman dan kuat yang berfungsi untuk melindungi data saat transit dan memungkinkan koneksi aman dipertahankan antara server dan klien.



Gambar 2. 6 Cara Kerja SSL
Sumber: (<https://www.jetorbit.com>, 2018)

Pada Gambar 2.6 menunjukkan cara kerja SSL secara sederhana. SSL dan TLS dapat meningkatkan keamanan protokol yang menggunakan TCP, tetapi merupakan metode akses HTTPS yang paling umum. HTTPS menyediakan situs web yang aman untuk aplikasi seperti e-niaga. Protokol SSL dan TLS memanfaatkan kriptografi kunci publik serta sertifikat kunci publik sebagai sarana untuk memastikan identitas dari subjek yang terlibat. Meskipun semakin banyak klien dan server yang kompatibel dengan TLS atau SSL dalam bentuk aslinya, beberapa *client* dan server tetap tidak mendukungnya. Dalam situasi ini, pengguna server atau klien dapat memanfaatkan produk SSL mandiri. Contohnya penggunaan *Stunnel* untuk menyediakan enkripsi SSL (Syahab, 2023).

6. *Cybercrime*

Cybercrime atau dalam latinnya kejahatan dunia maya merupakan kejahatan yang muncul karena dampak negatif dari perkembangan teknologi dengan media perantara seperti komputer, ponsel, serta perangkat lainnya yang dapat terhubung dengan internet. *Cybercrime* ini juga termasuk aktivitas yang melanggar hukum dimana kejahatan ini bersifat maya karena pelakunya tidak tampak secara fisik dan melakukannya secara ilegal (Siahaan, 2018).

Jenis *cybercrime* sedang meningkat saat ini melihat perkembangan teknologi juga semakin pesat. Hal ini menimbulkan metode dalam melakukan *cybercrime* cukup beragam diantaranya yaitu (Futra, 2020):

a. *Password Cracker*

Password cracker mencakup tindakan mengambil kata sandi orang lain dengan menggunakan program yang memiliki kemampuan tersebut. Tindakan ini juga biasa dilakukan untuk menonaktifkan sistem keamanan kata sandi.

b. *Spoofing*

Istilah “*spoofing*” dalam dunia maya mengacu pada penyamaran informasi untuk tujuan melakukan kejahatan siber (*cybercrime*). *Spoofing* merupakan tindakan memalsukan data atau identitas pribadi seseorang dengan tujuan agar pelaku dapat mengakses jaringan komputer seakan-akan bertindak sebagai pihak yang berwenang.

c. *DoS (Denial of Service Attack)*

DoS merupakan bentuk serangan yang menargetkan suatu perangkat selaku objek dari kejahatan ini dengan memakan sumber daya (*resources*) perangkat tersebut, sampai perangkat tidak berjalan secara optimal atau tidak dapat mengakses jaringan, sehingga memungkinkan pengguna lain untuk mengganggu komputer tersebut.

d. *Sniffing*

Tindak kejahatan yang tujuan utamanya untuk mengambil data atau informasi secara ilegal melalui perantara jaringan internet disebut dengan *sniffing*. *Sniffing* merupakan tindakan kriminal dimana pelaku mencuri nama pengguna beserta kata sandi milik orang lain dan menggunakan akun tersebut untuk melakukan penipuan atau merusak bahkan menghapus data milik orang tersebut.

7. *Packet sniffing*

Packet adalah sekumpulan informasi yang dikirim ke perangkat komputer, server, dan lain-lain yang melewati jaringan internet. *Sniffing* merupakan tindakan yang dilakukan untuk mengendus atau mengetahui isi *packet* tersebut. *Packet sniffing* adalah penggunaan *packet sniffer* untuk penyadapan paket data pada jaringan komputer. *packet sniffer* menggunakan metode penyerangan dengan memantau semua paket yang melewati media komunikasi apapun, baik itu melalui kabel atau nirkabel. Jika paket tersebut berhasil didapatkan, paket kemudian dapat diatur ulang dan data yang dikirim seseorang dapat diketahui oleh individu yang tidak berwenang. Ini dapat terjadi karena pada prinsipnya, semua koneksi *Ethernet* adalah koneksi siaran (*broadcast*), yang berarti semua perangkat di jaringan menerima paket yang dikirim oleh satu perangkat. Agar komputer terhindar dari serangan ini terbilang cukup sulit dikarenakan *packet sniffing* ini menggunakan pendekatan pasif dimana pihak penyerang tidak perlu melakukan tindakan apapun hanya mendengarkan (Hidayat, 2018).

Packet sniffing dapat dilakukan dalam beberapa cara dan menggunakan berbagai teknik untuk memantau dan merekam lalu lintas data dalam jaringan. Terdapat dua jenis serangan *packet sniffing* yaitu *sniffing* aktif dan *sniffing* pasif. Berikut penjelasan kedua jenis serangan *sniffing* tersebut:

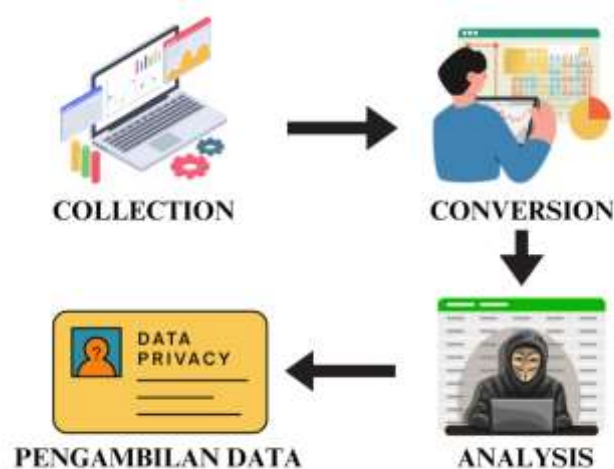
a. *Sniffing* Aktif

Sniffing aktif melibatkan intervensi dalam lalu lintas data untuk menyadapnya. Penyadap melakukan manipulasi pada lalu lintas, seperti mengalihkan lalu lintas atau memanipulasi tabel ARP, sehingga data yang

seharusnya ditujukan ke perangkat lain dapat diterima oleh penyadap. Sederhananya, *sniffing* aktif merupakan bentuk kejahatan siber dengan cara mengubah isi paket data. *Sniffing* aktif sering digunakan dalam serangan jaringan untuk mencuri informasi sensitif atau menyadap data dengan cara yang tidak sah. *Sniffing* aktif dilakukan pada *switch* jaringan, tidak menggunakan *hub*, dengan menyuntikkan lalu lintas ke LAN dengan berbagai cara.

b. *Sniffing* Pasif

Sniffing pasif adalah teknik penyadapan lalu lintas data dalam jaringan tanpa melakukan perubahan atau intervensi pada lalu lintas tersebut. Penyadap menggunakan perangkat atau perangkat lunak untuk mendengarkan dan merekam paket data yang melewati jaringan, tanpa mengganggu koneksi atau mengubah data yang sedang ditransfer. Berbeda dengan *sniffing* aktif, *sniffing* pasif dilakukan melalui *hub*. Semua data dari LAN ke LAN sebenarnya dikirim ke mesin yang menghubungkan keduanya terlebih dahulu. Jenis pengintaian ini menunggu data dikirim dan menyerang *hub* yang menghubungkan data dari LAN ke LAN.



Gambar 2. 7 Proses kerja *Sniffing*

Pada Gambar 2.7 Proses kerja *sniffing* adalah langkah-langkah yang dilakukan oleh perangkat lunak *sniffing* untuk memantau dan merekam lalu lintas data yang melewati jaringan. Proses *sniffing* melibatkan beberapa tahapan, mulai dari pengumpulan data hingga pengambilan data. Berikut adalah proses kerja *sniffing* secara umum (Qadeer, 2010).

a. Pengumpulan Data (*Collection*)

Sniffer menampung paket data yang melewati jaringan. Ini dapat dilakukan dengan berbagai cara, seperti mendengarkan lalu lintas pada jaringan fisik atau menangkap lalu lintas nirkabel pada jaringan Wi-Fi. *Sniffer* secara aktif mendeteksi dan merekam paket-paket data ini, baik yang dikirimkan secara broadcast di jaringan atau yang ditujukan untuk perangkat tertentu.

b. Konversi (*Conversion*)

Setelah paket data ditangkap, *sniffer* akan mengonversi informasi dalam paket tersebut ke dalam bentuk yang dapat dibaca dan dianalisis. Ini melibatkan penguraian informasi dalam paket, termasuk *header* dan informasi seperti alamat sumber, alamat tujuan, jenis data, dan lainnya. Data yang terkumpul biasanya berupa urutan bit atau *byte* yang tidak bisa dipahami dengan mudah oleh manusia. Oleh karena itu, konversi diperlukan untuk memahami isi paket.

c. Analisis (*Analysis*)

Sniffer dapat melakukan analisis terhadap data yang telah terkumpul. Ini melibatkan pemantauan, pemrosesan, dan interpretasi data yang ditangkap. Selama tahap analisis, *sniffer* menganalisis paket data untuk berbagai tujuan. Ini bisa meliputi pemantauan kinerja jaringan, identifikasi ancaman keamanan,

pemecahan masalah jaringan, atau pengejaran aktivitas tertentu. Analisis ini dapat dilakukan secara *real-time*, dimana hasil analisis dapat digunakan untuk mengambil tindakan segera, atau data dapat disimpan untuk analisis lebih lanjut.

d. Pengambilan Data (*Action*)

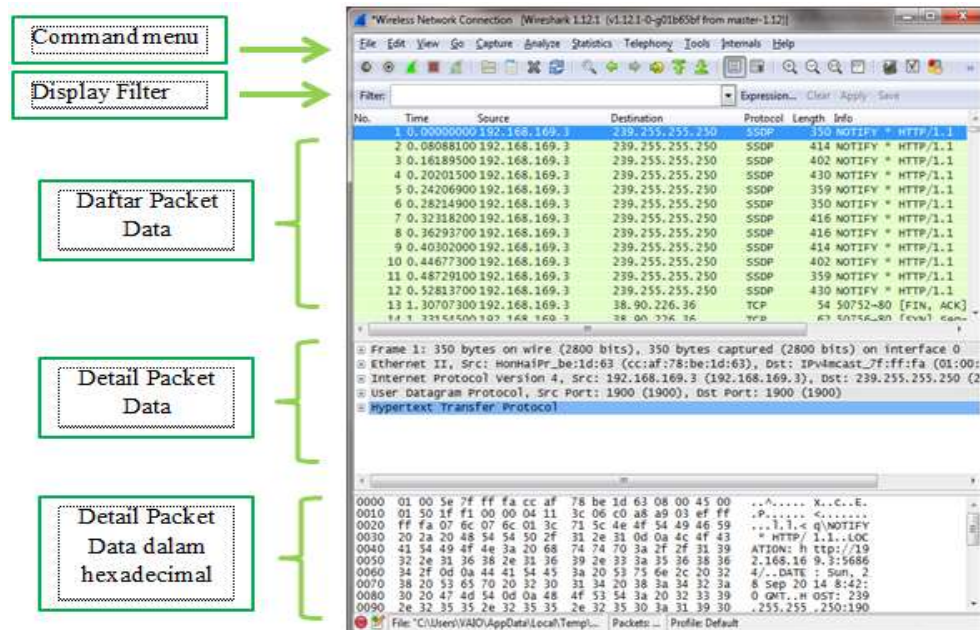
Pada tahap pengambilan data, informasi yang relevan dari paket-paket yang telah dianalisis dapat diambil untuk penggunaan selanjutnya. Ini bisa berupa penyimpanan data log, pelaporan, atau tindakan respons lainnya sesuai dengan tujuan *sniffing* tersebut. Dalam beberapa kasus, data yang telah diambil dapat digunakan untuk tujuan yang bermasalah atau ilegal, seperti pencurian informasi sensitif, jika digunakan oleh pihak yang tidak sah.

8. *Wireshark*

Wireshark adalah perangkat lunak perekam dan analisis lalu lintas jaringan yang bersifat terbuka (*Open Source*). Perangkat lunak ini memungkinkan pengguna untuk menangkap data yang melintasi jaringan, memahami struktur dan isi paket, serta menganalisis protokol yang digunakan dalam lalu lintas jaringan. Dengan *Wireshark*, pengguna dapat menyelidiki masalah jaringan, menganalisis keamanan, dan memahami bagaimana aplikasi dan perangkat berkomunikasi melalui jaringan (Abdillah, 2020).

Wireshark memiliki beberapa fitur utama yang dapat membantu pengguna untuk mengidentifikasi masalah atau kerentanan keamanan diantaranya:

- 1) *Packet Capture*, fitur yang dapat menangkap paket data dari berbagai antarmuka jaringan, baik yang terhubung secara kabel maupun nirkabel.
- 2) *Packet Analysis*, fitur ini memungkinkan pengguna untuk memeriksa isi setiap paket data, termasuk *header protocol* dan *payload*.
- 3) *Filtering*, dengan *Wireshark* pengguna dapat menerapkan filter untuk menampilkan hanya paket data yang sesuai dengan kriteria tertentu, dan membantu untuk fokus pada informasi yang relevan.
- 4) *Protocol Decoding*, perangkat lunak ini memiliki kemampuan untuk mendekode berbagai protokol jaringan yang digunakan dalam paket data, memungkinkan pengguna memahami interaksi antara perangkat dan aplikasi.
- 5) *Statistics*, dengan fitur ini juga dapat menampilkan statistik terkait jumlah paket, protokol yang paling banyak digunakan, alamat IP yang paling aktif, dan sebagainya.
- 6) *Export Data*, hasil analisis dapat diekspor ke berbagai format, seperti file PCAP (*Packet Capture*) yang dapat dibuka dengan *Wireshark* di komputer lain.



Gambar 2. 8 Wireshark Interfaces
Sumber: (<https://www.kompasiana.com>, 2015)

Wireshark digunakan oleh para profesional keamanan jaringan, administrator sistem, analis jaringan, dan peneliti keamanan untuk mengidentifikasi masalah jaringan, melacak serangan, memeriksa komunikasi jaringan yang mencurigakan, dan menganalisis protokol secara mendalam. Penting untuk diingat bahwa penggunaan *Wireshark* harus dilakukan dengan etika dan sesuai hukum. Menangkap lalu lintas jaringan tanpa izin yang sesuai atau tanpa hak akses yang sah dapat melanggar privasi dan undang-undang keamanan data.

9. Ettercap

Alberto Omaghi (AloR) dan Marco Valleri (NaGa) menciptakan *tools Ettercap* menjadi sebuah perlengkapan untuk penyerangan “*Man-in-the-Middle*” pada jaringan. *Ettercap* adalah alat keamanan jaringan yang dikenal karena kemampuannya untuk melakukan serangan MitM dan menganalisis lalu lintas jaringan. *Ettercap* memposisikan dirinya sebagai “penengah” yang

memungkinkannya merumuskan serangan terhadap protokol ARP. Berada dalam posisi tersebut, *tools* ini memungkinkan pengguna memantau komunikasi jaringan secara *real time*, menganalisis protokol yang digunakan seperti HTTP, FTP, POP, dan SSH1, dan dapat memanipulasi data dalam lalu lintas. Lebih parahnya *tools* ini juga dapat menyebarkan sertifikat SSL palsu dalam bagian HTTPS pada korban.

Adapun fitur dari *tools Ettercap* yaitu:

- 1) Serangan *Man-in-the-Middle (MitM)*, fitur ini memungkinkan pengguna untuk memposisikan diri sebagai perantara antara dua pihak yang berkomunikasi sehingga dapat memantau atau bahkan memanipulasi data yang mereka kirimkan.
- 2) Protokol Analisis, dengan fitur ini dapat menganalisis berbagai protokol jaringan, seperti ARP, DNS, HTTP, dan lain sebagainya. Ini dapat memberikan bantuan kepada pengguna untuk memahami interaksi antara perangkat dalam jaringan.
- 3) Deskripsi Paket, *Ettercap* dapat membongkar dan menampilkan isi dari paket data yang lewat melalui jaringan, termasuk informasi seperti *header* protokol dan *payload*.
- 4) *Filtering*, dengan fitur ini dapat menerapkan filter untuk menangkap dan memonitor lalu lintas yang relevan untuk tujuan penelitian atau analisis.
- 5) *Session Hijacking*, *Ettercap* memungkinkan pengguna untuk mengambil alih sesi atau koneksi yang ada antara perangkat dalam jaringan. Hal ini digunakan untuk tujuan analisis dan serangan.

B. Kajian Penelitian yang relevan

Beberapa studi sebelumnya yang berkaitan dengan penelitian yang akan dilaksanakan sangat penting untuk digunakan sebagai sumber acuan. Oleh sebab itu, penelitian ini bertujuan untuk menghindari duplikasi dan plagiarisme, serta sebagai bentuk pengembangan penelitian-penelitian sebelumnya yang memiliki topik serupa.

Pada tahun 2019, penelitian yang dilakukan oleh Saputra dalam riset berjudul "Analisis Keamanan Jaringan Nirkabel dengan Pendekatan Wardriving di Kampus STIMIC MIC Cikarang" mengindikasikan bahwa ada sejumlah masalah yang berhasil terdeteksi pada jaringan LAN dan WLAN (Wireless Local Area Network) di kampus tersebut. Hal ini menimbulkan celah keamanan pada konfigurasi *IP address* dalam kampus STIMIC MIC Cikarang karena siapa saja yang berada dilingkungan kampus berpotensi mendapatkan akses ke jaringan kampus. Dalam penelitian ini penulis memanfaatkan metode *Wardriving* yang berguna untuk memetakan *access point* sebagai perluasan dari jaringan kabel LAN utama, yang bertujuan untuk mengakomodasi pengguna yang menggunakan perangkat nirkabel. Penulis memanfaatkan alat Android Debug Bridge (ADB) untuk mengidentifikasi perangkat Android yang telah terhubung dan disambungkan dengan komputer. Lalu, menjalankan *BlueNmea* pada android agar terkoneksi dengan GPS. Kemudian jika sudah terkoneksi, penulis menggunakan aplikasi *Kismet* yang berperan untuk mengidentifikasi semua jaringan nirkabel yang tidak memiliki jaringan Wi-Fi tersembunyi (SSID tersembunyi) dan memungkinkan paket data untuk berpindah masuk dan keluar., serta untuk melihat *hotspot* dalam

lingkungan tersebut. Setelah itu, *Giskimet* akan mengkonversi file *log Kismet* dari hasil *Wardriving* menjadi sebuah *database* berisikan Wi-Fi dan membuat file berekstensi KML lalu melakukan pemetaan dengan mengakses file *kismet* menggunakan *Google Earth*. Dari hasil pemetaan ditemukan 11 buah Wi-Fi dengan enkripsi, dan sebanyak 3 buah yang tidak menggunakan enkripsi yang terdeteksi di area Kampus STIMIC MIC Cikarang dengan hasil *Wardriving* yang berbeda seperti *None Encryption*, WEP, dan WPA2.

Desi Maya Sari, Muh. Yamin, dan LM. Bahtiar Aksara melakukan penelitian pada tahun 2017 tentang “Analisis Sistem Keamanan Jaringan *Wireless* (WEP, WPA PSK/WPA2PSK) *Mac Address*, Menggunakan Metode *Penetration Testing*”. Metode penetrasi yang dimanfaatkan dalam penelitian ini dengan bantuan *tools aircrack* untuk *cracking* WEP dan WPA PSK/WPA2PSK serta untuk *mac address filtering* menggunakan *tools macchanger* dengan sistem operasi Kali Linux yang dikerjakan di Jurusan Teknik Informatika Fakultas Teknik UHO. Peneliti melakukan pengujian dengan dua jenis serangan yaitu serangan *cracking the encryption* dan serangan *bypassing WLAN authentication* untuk menguji tipe keamanan jaringan *Wireless* yang baik diterapkan pada kampus tersebut. Pada serangan mengenai enkripsi tipe keamanan WEP, tiga uji coba berhasil mengatasi tiga kombinasi yang berbeda (termasuk 'huruf dan angka', 'huruf', dan 'huruf, angka, dan simbol') dan password yang beragam. Sementara itu, pada tipe keamanan WPA dan WPA2PSK teridentifikasi gagal dilakukan pada uji coba pertama dan ketiga dengan kombinasi 'huruf dan angka' serta 'huruf, simbol, dan angka', hanya uji coba kedua yang berhasil disusupi oleh jenis serangan *cracking the*

encryption. Kemudian, tipe keamanan Filtering berdasarkan alamat MAC berhasil diatasi dengan serangan yang melewati autentikasi WLAN. Oleh karena itu, sistem keamanan yang paling sesuai untuk digunakan dalam jaringan nirkabel adalah WPAPSK/WPA2PSK.

Sebelumnya, Aditya Ariyanto, dan Asmunin juga telah melakukan penelitian tentang “Deteksi Packet *Sniffing* Pada *Wireless* Menggunakan ARPWatch” pada tahun 2018. Pada penelitian ini memanfaatkan aplikasi *Arpwatch* yang akan berfungsi untuk mendeteksi serangan pada jaringan yang bersifat publik, lalu akan memantau aktivitas *Ethernet* serta megumpulkan data yang diterima dalam format pasangan alamat IP dan MAC. *Arpwatch* digunakan dalam mengidentifikasi tindakan *packet sniffing* yang mengindikasikan *Arp Spoof*. Untuk mengaktifkan *arpwatch* sehingga dapat memonitor jaringan harus melakukan konfigurasi pada *arpwatch*. Sehingga, ketika terjadi serangan packet sniffing pada jaringan internet, *arpwatch* secara otomatis akan memberikan pemberitahuan. Meskipun dilakukan percobaan berulang kali, peneliti berhasil melakukan percobaan serangan menggunakan *arp* pada sistem operasi Ubuntu.

Penelitian dengan judul “Analisis Keamanan Jaringan Wi-Fi Terhadap Serangan *Packet sniffing* di Universitas PGRI Sumatera Barat” telah dilakukan oleh Fatimah, pada tahun 2022. Pada penelitian ini menggunakan *tools* dari kali linux yaitu *Wireshark*, dan *Ettercap* dimana pengujian yang dilakukan pada beberapa gedung yang berada di area kampus Universitas PGRI Sumatera Barat dan beberapa situs yang sering digunakan mahasiswa. Hasil dari penelitian ini jaringan Wi-Fi di kampus tersebut sudah mengimplementasikan enkripsi WPA2 dan telah dianggap

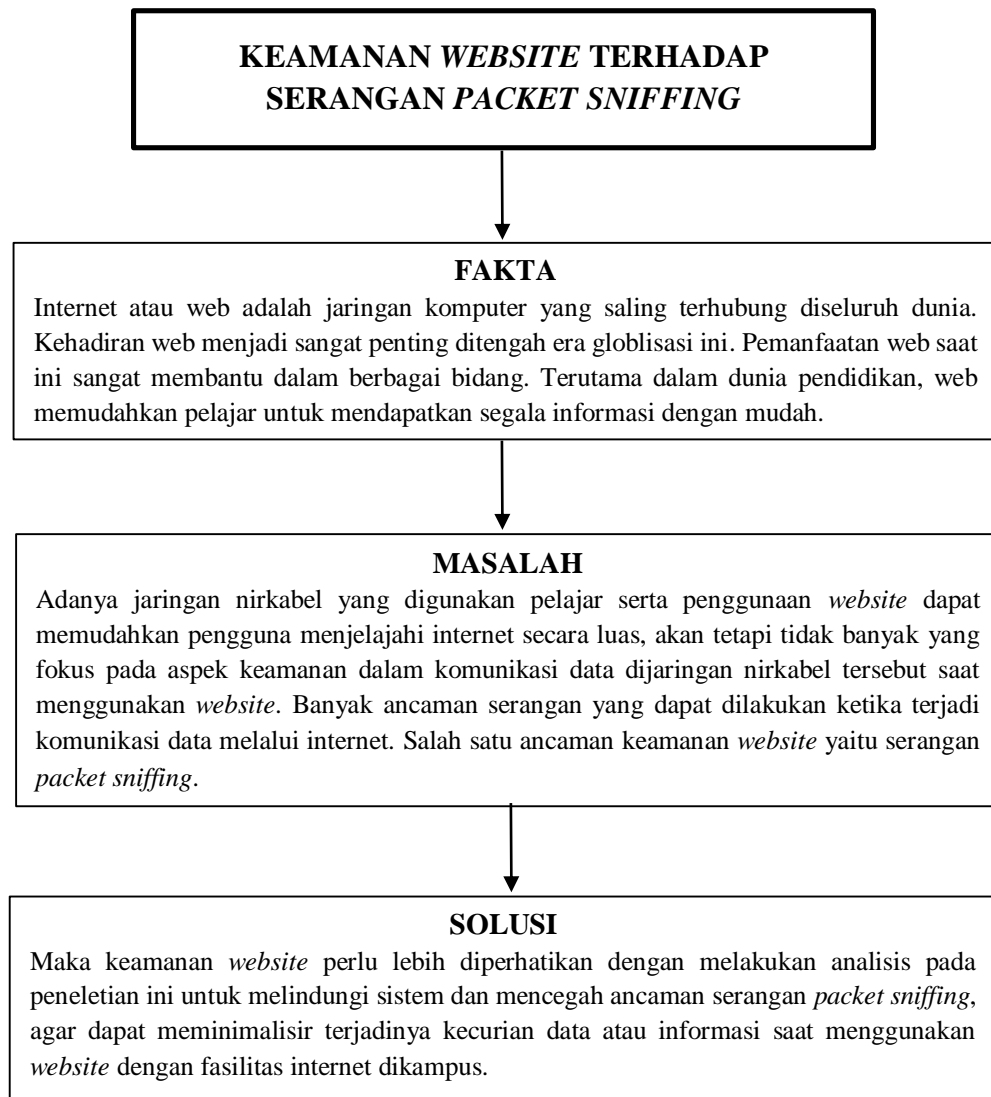
terlindungi dari serangan yang telah dilakukan pengujian dengan serangan *packet sniffing*. Hal ini terbukti karena pada saat melakukan serangan *packet sniffing*, peneliti tidak bisa mendapatkan *IP Address* dari laptop pengujian. Sementara pada situs-situs yang diuji, peneliti dapat menangkap data pada situs yang menggunakan protokol HTTP, sedangkan situs yang menggunakan protokol HTTPS peneliti tidak dapat menangkap data tersebut.

Penelitian lain yang menggunakan *tools Ettercap* untuk melakukan pengujian dilakukan oleh Hidayat, pada tahun 2018 yang berjudul “Analisis Keamanan Jaringan Pada Fasilitas Internet (Wi-Fi) Gratis Terhadap Serangan *Packet sniffing*”. Dalam penelitian ini, peneliti melakukan identifikasi keamanan Wi-Fi dengan bantuan aplikasi *Wi-Fite* yang berfungsi untuk melakukan pemindaian *hotspot* yang berada dilingkungan laptop penyerang serta dapat menampilkan informasi keamanan yang digunakan pada jaringan Wi-Fi. Kemudian, untuk menganalisa *client* yang terhubung pada satu *hotspot* menggunakan *tools Ettercap*. Peneliti memperoleh nilai tingkat kelemahan pada 4 lokasi yang dijadikan penelitian yang sering digunakan oleh pengguna di Universitas Siliwangi, dimana hasil keseluruhan menunjukkan rata-rata tingkat kerentanan terjadinya serangan adalah 0,6. Artinya, keamanan jaringan Wi-Fi yang berada di area kampus termasuk dalam rentan kelemahan yang tinggi dan banyaknya pengguna jaringan Wi-Fi gratis tersebut yang tidak memahami akan banyaknya masalah pada jaringan yang lemah.

Tabel 2. 2 Kajian Pustaka

No	Peneliti	Judul	Metode	Persamaan	Perbedaan
1	Saloko Cahyo Saputro, <i>et al.</i> , (2019)	Analisis Keamanan Jaringan <i>Wireless</i> Menggunakan Metode <i>Wardriving</i> Pada Kampus STIMIK MIC Cikarang	<i>Wardriving</i>	Menganalisa keamanan jaringan <i>Wireless</i>	Metode yang digunakan berbeda
2	Desi Maya Sari, <i>et al.</i> , (2017)	Analisis Sistem Keamanan Jaringan <i>Wireless</i> (WEP, WPA PSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration Testing.	<i>Penetration Testing</i>	Menganalisa keamanan jaringan <i>Wireless</i>	Metode yang digunakan berbeda
3	Aditya Ariyanto dan Asmunin (2018)	Deteksi <i>Packet sniffing</i> pada <i>Wireless</i> Menggunakan Arp Watch	<i>Arp Watch</i>	Menganalisa keamanan jaringan <i>Wireless</i> untuk mencegah serangan <i>packet sniffing</i> .	Metode yang digunakan berbeda
4	Fatima (2022)	Analisis Keamanan Jaringan Wi-Fi Terhadap Serangan <i>Packet sniffing</i> di Universitas PGRI Sumatera Barat	<i>Penetration Testing</i>	Menganalisa keamanan suatu jaringan <i>Wireless</i> untuk mencegah serangan <i>packet sniffing</i> .	Objek yang digunakan berbeda.
5	Hidayat (2018)	Analisis Keamanan Jaringan Pada Fasilitas Internet (Wi-Fi) Gratis Terhadap Serangan <i>Packet sniffing</i>	<i>Penetration Testing</i>	Menganalisa keamanan suatu jaringan <i>Wireless</i> agar dapat mengantisipasi serangan <i>packet sniffing</i> .	Objek yang digunakan berbeda.

C. Kerangka Pikir



Gambar 2. 9 Kerangka Pikir

Internet atau web adalah jaringan komputer yang saling terhubung diseluruh dunia. Kehadiran web menjadi sangat penting ditengah era globlisasi ini. Pemanfaatan web saat ini sangat membantu dalam berbagai bidang. Terutama dalam dunia pendidikan, web memudahkan pelajar untuk mendapatkan segala informasi dengan mudah. Universitas Negeri Makassar adalah salah satu kampus

yang memanfaatkan layanan jaringan nirkabel dan penggunaan *website* sebagai fasilitas untuk memudahkan mengakses informasi dan menuntut ilmu.

Jaringan yang terhubung ke internet pada prinsipnya memiliki kerentanan dan dapat dimanfaatkan oleh para pelaku kejahatan dunia maya. Hal ini disebabkan oleh sifat dasar jaringan yang melibatkan pertukaran informasi, yang mungkin dapat diakses oleh pihak yang tidak berwenang. Adanya penggunaan *website* dapat memudahkan pengguna menjelajahi internet secara luas, akan tetapi tidak banyak yang memperhatikan keamanan komunikasi data pada jaringan nirkabel tersebut saat menggunakan *website*. Ada banyak potensi ancaman serangan yang dapat dilakukan ketika terjadi komunikasi data melalui internet. Salah satu ancaman keamanan *website* yaitu serangan *packet sniffing*.

Maka keamanan *website* perlu lebih diperhatikan dengan melakukan analisis melalui penelitian ini untuk melindungi dan mencegah ancaman serangan *packet sniffing* terhadap sistem, serta dapat meminimalisir terjadinya pencurian data atau informasi saat menggunakan *website* dengan menggunakan jaringan nirkabel di kampus Universitas Negeri Makassar Fakultas Teknik. Penulis memanfaatkan aplikasi *Wireshark* untuk melakukan analisis, dan *tools Ettercap* untuk melakukan *sniffing*. Hal ini bertujuan untuk mengetahui tingkat kerentanan keamanan *website* dari serangan *packet sniffing*.

BAB III

METODE PENELITIAN

A. Jenis Penelitian

Jenis penelitian ini ialah menggunakan metode eksperimental. Dimana penelitian eksperimental merupakan salah satu jenis penelitian yang mengkaji pengaruh suatu perlakuan terhadap objek untuk mengetahui akibat yang ditimbulkan (Arini, 2010). Objek yang akan diteliti akan diberikan suatu eksperimen berupa serangan *packet sniffing* menggunakan *tools Ettercap* kemudian dilakukan pengamatan terhadap kondisi-kondisi yang didapatkan dengan aplikasi *Wireshark* untuk dapat diketahui kerentanan terjadinya suatu serangan pada objek tersebut.

B. Waktu dan Tempat Penelitian

1. Waktu Penelitian

Penelitian ini dilakukan dalam rentan waktu dari bulan Juni hingga bulan September tahun 2023.

2. Tempat Penelitian

Penelitian dilaksanakan di Lab Jaringan Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar.

C. Teknik Pengumpulan Data

Pengumpulan data merupakan tindakan dimana mengubah data penelitian menjadi sesuatu yang dapat dikembangkan lalu dapat dimanfaatkan untuk menjawab rumusan masalah, sehingga dapat menghasilkan sebuah kesimpulan

yang kompleks. Dalam penelitian ini, digunakan berbagai metode untuk mengumpulkan data sebagai berikut:

1. Studi literatur

Pada tahap studi literatur, dilakukan analisis dengan cara mengumpulkan materi yang terkait dengan *website*, jaringan nirkabel/Wi-Fi, dan serangan *packet sniffing* yang bersumber dari beberapa jurnal, buku, hasil *browsing* internet, serta orang yang berpengetahuan mengenai hal tersebut.

2. Observasi

Observasi dilakukan pada beberapa *website* yang sering digunakan mahasiswa di Fakultas Teknik Universitas Negeri Makassar diantaranya SIMPEL, SIM-TA, IDS, Sigmatik, dan SIPI.

D. Teknik Analisis Data

Peneliti menganalisis data yang diperoleh dari pengamatan dengan aplikasi *Wireshark* menggunakan pendekatan deskriptif kualitatif, dimana metode analisis ini dilakukan dengan cara membandingkan keamanan *website* dari situs yang diuji guna mencapai hasil yang akurat dari penelitian yang telah dilaksanakan.

E. Alat dan Bahan

Dibutuhkan beberapa instrumen untuk mendukung kelancaran proses penelitian ini yaitu sebagai berikut:

1. Perangkat Keras

Dalam proses penelitian perangkat keras (*hardware*) yang digunakan yaitu:

- a. Laptop Asus VivoBook 14 X407MA Prosesor Intel inside RAM: 4GB
- b. *Wireless Fidelity*

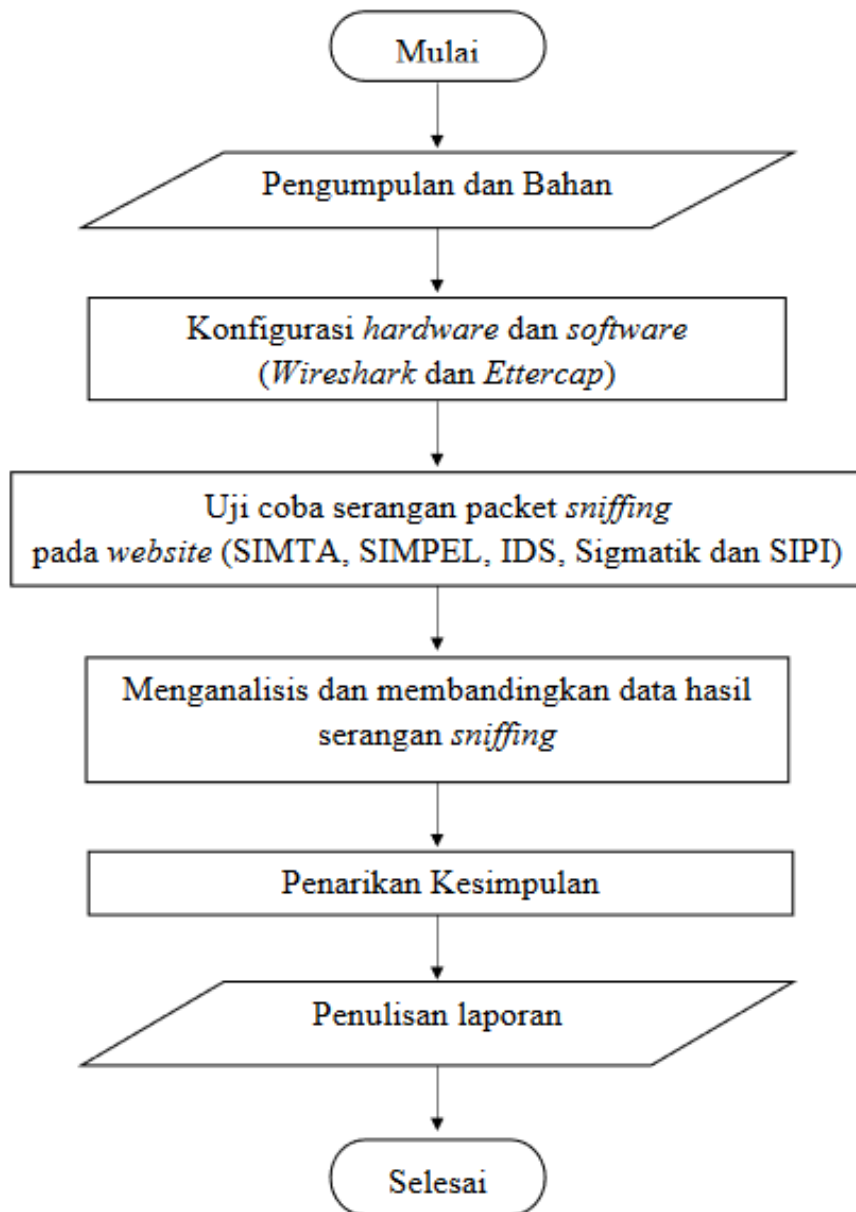
2. Perangkat Lunak

Dalam proses penelitian perangkat lunak (*software*) yang dibutuhkan yaitu:

- a. Sistem Operasi Kali Linux
- b. Aplikasi *Wireshark* (digunakan untuk serangan *packet sniffing*)
- c. Aplikasi *Ettercap* (digunakan untuk serangan *poisoning*)
- d. Website JTIK (SIMPEL, SIM-TA, IDS, Sigmatik, dan SIPI)

F. Prosedur Penelitian

Untuk mempermudah pemahaman dalam penelitian diperlukan prosedur penelitian yang disajikan dalam bentuk diagram alur penelitian berikut:



Gambar 3. 1 Alur Penelitian

Berdasarkan Gambar 3.1 Alur Penelitian, penelitian ini dilakukan dalam beberapa tahapan. Tahap-tahapan tersebut meliputi:

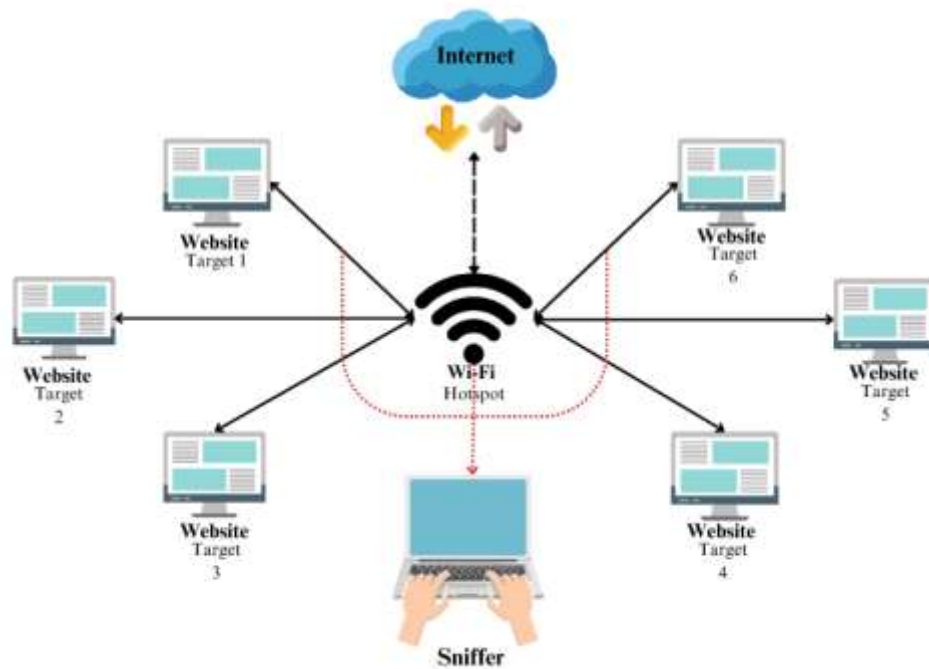
1. Mengumpulkan dan mempelajari studi literatur dari berbagai referensi yang bersifat relevan. Referensi ini dikumpulkan oleh peneliti dari berbagai sumber

seperti buku-buku akademik, laporan penelitian sebelumnya, artikel, jurnal, dan tesis yang dapat menunjang penelitian ini.

2. Menyiapkan semua perangkat keras dan perangkat lunak yang diperlukan agar penelitian dapat dilakukan dengan lancar. Pada proses ini, penulis menggunakan bantuan aplikasi seperti *Wireshark*, dan *Etercap* untuk melakukan analisis jaringan serta serangan *packet sniffing*.
3. Kemudian melakukan sebuah percobaan serangan *sniffing* pada *website* SIMTA, SIMPEL, IDS, Sigmatik, dan SIPI yang terkoneksi di jaringan nirkabel (Wi-Fi) juga terkoneksi dengan pengguna.
4. Menganalisis data yang dapat diperoleh dari pengujian serangan *sniffing* dan melakukan perbandingan tingkat keamanan setiap *website* terhadap proses *sniffing*.
5. Membuat kesimpulan berdasarkan semua data yang telah dikumpulkan, dan memberikan solusi untuk ditindak lanjuti agar dapat digunakan untuk meminimalisir terjadinya serangan *packet sniffing* pada situs *website* yang sering digunakan.

G. Rancangan Penelitian

Selanjutnya, penulis membuat rancangan penelitian sebelum melakukan pengujian. Sehingga, dapat mempermudah pelaksanaan pengujian pada penelitian yang dilakukan. Berikut skema atau topologi yang akan dilakukan peneliti.



Gambar 3. 2 Skema Penelitian

Pada skema tersebut menampilkan sejumlah perangkat komponen yang saling terhubung satu sama lain meliputi jaringan internet yang berasal dari Wi-Fi sebagai *hotspot* lalu terkoneksi dengan situs-situs web yang sedang melakukan transmisi data. Pada saat terjadinya proses transmisi data antar target dan *hotspot*, *sniffer* secara diam-diam dapat memantau dan menangkap semua paket data tersebut.

Adapun Tabel 3.1 Hasil Observasi yang telah dirancang oleh penulis berisi informasi tentang apa yang ditemukan atau diamati selama pengujian berlangsung sebagai berikut:

Tabel 3. 1 Hasil Observasi

Website	Informasi	Hasil Analisis	Keterangan
SIMPEL	Jenis pesan		POST, GET
	<i>Host</i>		Yang bertindak sebagai server
	Jenis koneksi		Penggunaan protokol enkripsi (SSL/TLS)
	Jenis konten		Perlindungan cookie (HttpOnly, Secure)
	Penggunaan aplikasi		<i>Web browser</i> yang digunakan
	Komunikasi		Bahasa yang diterima server
	Uji <i>Man in the Middle</i> (MitM)		Respons terhadap serangan <i>Man in the Middle</i>
	Waktu		Waktu ketika server mengirimkan data
	Server		Jenis server yang digunakan
	Data sensitif		Jenis data yang dikirim (<i>login</i> , informasi pribadi, dll)

Beberapa parameter yang dapat menunjang penelitian ini seperti situs *website* yang dikunjungi yang akan dianalisa tingkat dan keamanan dan kerentanan terjadi serangan berdasarkan berhasil tidaknya menangkap data berupa informasi *Username*, dan *password* saat melakukan serangan *packet sniffing*. Jaringan internet atau *hotspot* yang digunakan, serta akun yang menggunakan perangkat yang berbeda-beda. Berikut merupakan skenario dari penelitian ini:



Gambar 3. 3 Skenario Penelitian

Ketika perangkat yang dijadikan peneliti sebagai target terkoneksi dengan *hotspot* tersebut. Kemudian melakukan *login* pada *website* SIMPEL, SIM-TA, IDS, Sigmaik, dan SIPI, maka terjadi proses transmisi data secara bolak-balik. Laptop penyerang yang juga terkoneksi dengan jaringan yang sama melakukan *sniffing* melalui aplikasi *Wireshark* dan bantuan *Ettercap* untuk mengetahui informasi *login* yang digunakan pada laptop target. Penulis melakukan serangan secara berulang-ulang pada ke-5 *website* tersebut menggunakan akun dan perangkat yang berbeda-beda hingga mendapatkan hasil yang valid. Hasil pengujian dari penelitian tersebut direalisasikan pada Tabel 3.2 Hasil Pengujian pada *Website* berikut:

Tabel 3. 2 Hasil Pengujian pada *Website*

Jaringan (Gateway)	Website yang Diuji	Akun (Target)	Hasil Penelitian	Keterangan
<i>Hotspot 1</i>	<ul style="list-style-type: none"> - SIMPEL - IDS - SIMTA - Sigmatik - SIPI 	IP Address pengguna	Data yang berhasil di <i>capture</i>	Aman/ rentan terhadap serangan
<i>Hotspot 2</i>	<ul style="list-style-type: none"> - SIMPEL - IDS - SIMTA - Sigmatik - SIPI 	IP Address pengguna	Data yang berhasil di <i>capture</i>	Aman/ rentan terhadap serangan

BAB IV

HASIL DAN PEMBAHASAN

Agar dapat mengevaluasi sejauh mana tingkat keamanan yang diterapkan pada *website* yang ada di Jurusan Teknik Informatika dan Komputer UNM, maka perlu dilakukan analisis. Sebagaimana yang umumnya diketahui, keamanan tidak hanya bergantung pada aplikasi *website* yang ada, melainkan pada aspek keamanan yang muncul selama proses pertukaran data antara *client* dan *web server* dalam suatu jaringan. Selain itu, juga terdapat banyak mahasiswa, dosen, dan staff yang masih kurang memahami tentang konsep *sniffing* dalam jaringan komputer.

A. Hasil Penelitian

Dalam analisis ini, melibatkan beberapa perangkat komponen yang terhubung, termasuk jaringan internet, titik akses Wi-Fi yang berasal dari *access point*, laptop penyerang, dan juga *website-website* yang menjadi target. Langkah berikutnya adalah melakukan pengujian keamanan dengan tujuan untuk mendapatkan pemahaman tentang masalah keamanan yang mungkin ada pada saat mengakses *website*.

1. Menghubungkan laptop ke jaringan internet. Dalam hal tersebut, peneliti memanfaatkan titik akses Wi-Fi yang berasal dari *access point* yang berada di ruangan Lab JTIK.



Gambar 4. 1 Koneksi Jaringan Nirkabel

2. Untuk memulai *Ettercap* di Kali Linux, klik “*Applications*” pada menu selanjutnya, pilih “*Sniffing & spoofing*” kemudian klik “*Ettercap Graphical*”. Alternatif lain dapat diakses melalui terminal dengan mengetikkan “*sudo Ettercap -G*”. Lalu akan ditampilkan Gambar 4.2 Tampilan *Interfaces Ettercap*.



Gambar 4. 2 Tampilan *Interfaces Ettercap*

3. Mengaktifkan “*Sniffing at Startup*” terlebih dahulu, kemudian memilih “eth0” sebagai *interface* yang akan digunakan. Lalu klik tanda centang untuk memulai *sniffing* dan akan menghasilkan tampilan awal pada Gambar 4.3 Memulai *Sniffing*.



Gambar 4. 3 Memulai *sniffing*

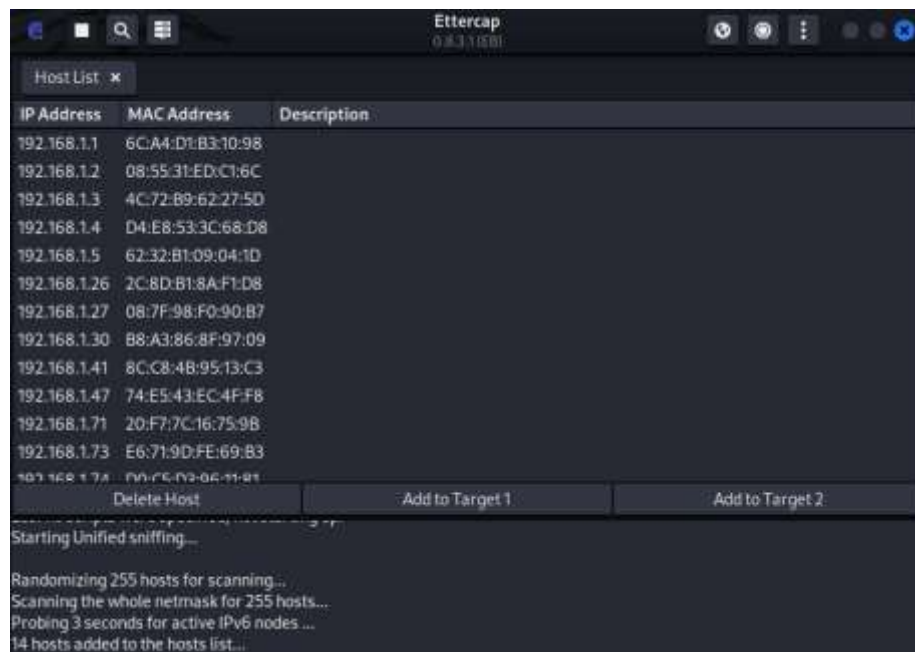
4. Melaksanakan *scanning* pada *host* yang terhubung dalam jaringan yang sama dengan mengklik opsi “*Host*” terlebih dahulu, kemudian memilih “*Scan for hosts*” lalu centang “*Enable IPv6 Scan*” dan tunggu hingga proses *scanning* selesai. Setelah proses *scanning* selesai, jumlah *host* yang terhubung dalam jaringan yang sama dengan penyerang akan ditampilkan pada Gambar 4.4 *Scanning Host* yang Terkoneksi.



Gambar 4. 4 *Scanning Host* yang terkoneksi

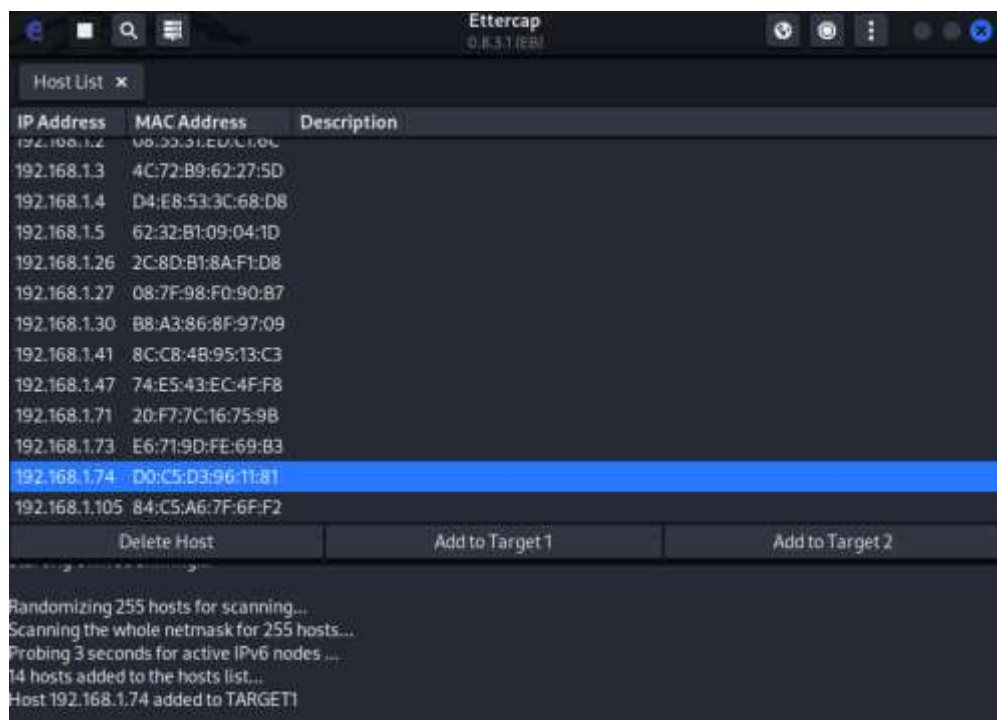
Pada Gambar 4.4 *Scanning Host* yang terkoneksi Menampilkan 14 *hosts* terkoneksi dalam jaringan tersebut.

- Menampilkan *list host* yang telah dipindai dengan cara meng-klik “*Hosts*”, lalu memilih “*Host List*”. Hasilnya yaitu ditampilkan *list host* seperti pada Gambar 4.5 *List Host* Broadband_UNM dibawah ini.



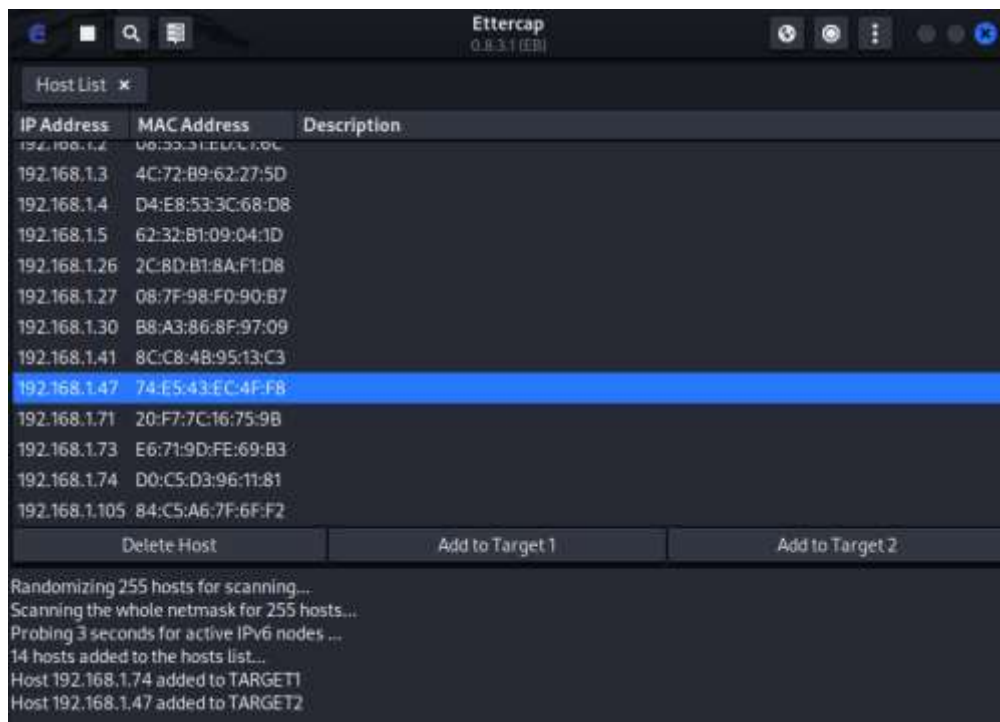
Gambar 4. 5 *List Host* Broadband_UNM

6. Dalam menjalankan *ARP Poisoning*, langkah awal adalah memilih *gateway* dan target dengan memeriksa alamat IP. Langkah berikutnya adalah memilih IP Address dari 192.168.1.1 sebagai Target 1 dengan meng-klik alamat IP tersebut dan memilih opsi “*Add to Target 1*”. Hal ini dilakukan karena alamat IP tersebut merupakan alamat *gateway*.



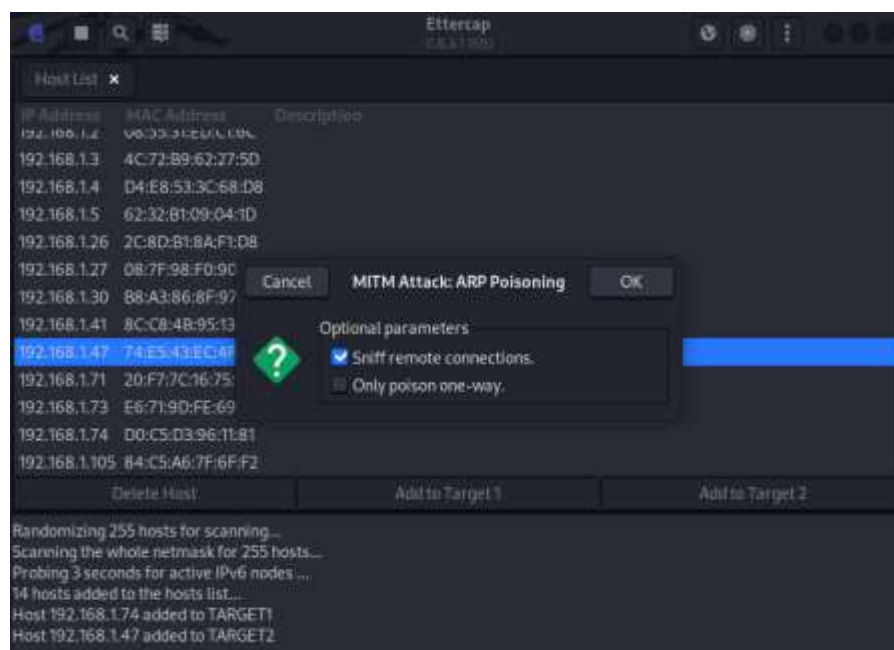
Gambar 4. 6 target 1 *gateway*

7. Selanjutnya, menetapkan IP Address 192.168.1.47 sebagai target 2 dengan mengklik alamat IP tersebut dan memilih opsi “*Add to Target 2*”. Tindakan ini diambil karena alamat IP tersebut merupakan alamat IP dari korban.

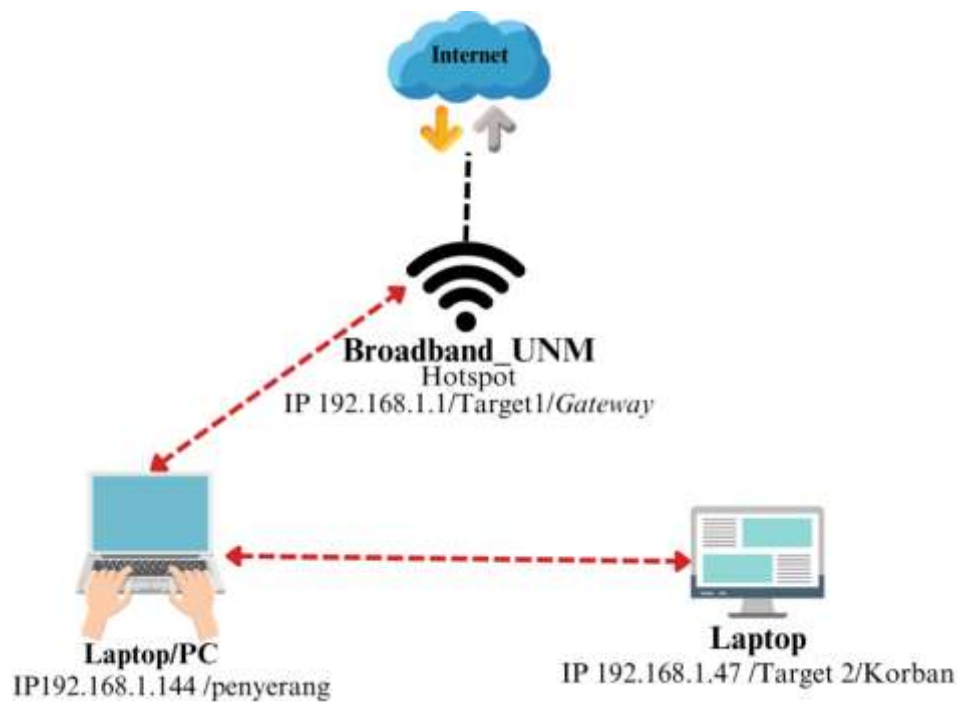


Gambar 4. 7 Menentukan target 2

8. Melakukan eksekusi ARP *Poisoning* dengan meng-klik opsi “MitM” lalu pilih “ARP *Poisoning*” dan mengaktifkan “*Sniff remote connections*” dengan memberi tanda centang lalu klik “OK”.

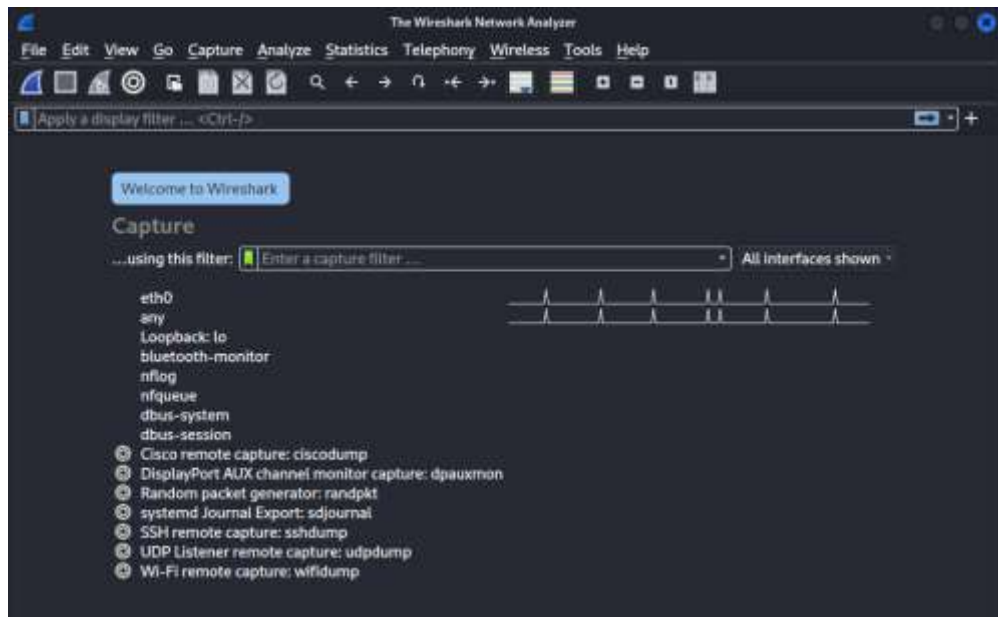
Gambar 4. 8 ARP *Poisoning*

9. Lalu, memulai proses *sniffing* dengan cara meng-klik “*Start Sniffing*”.
10. Apabila serangan MitM (ARP *Poisoning*) berhasil dijalankan, proses transfer data dari laptop target ke *hotspot* atau sebaliknya akan melalui laptop penyerang. Ilustrasinya seperti yang tampak pada Gambar 4. 9 Proses Transmisi Data berikut.



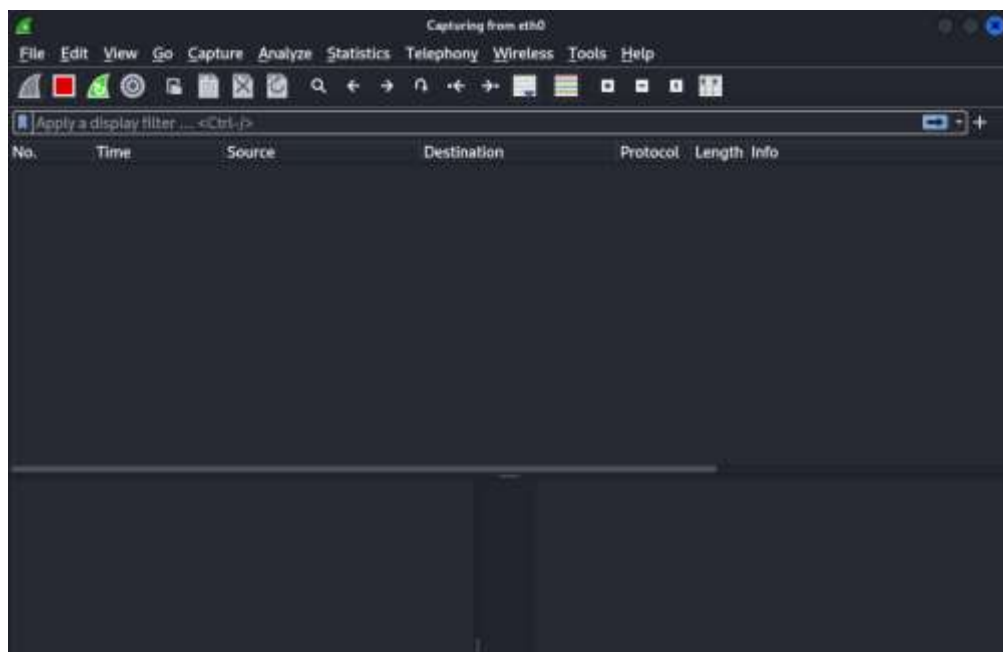
Gambar 4. 9 Proses Transmisi Data

11. Buka aplikasi *Wireshark* di Kali Linux dengan cara pilih “*Applications*” lalu pilih “*Sniffing & spoofing*” kemudian klik “*Wireshark*”. Hal ini akan menghasilkan tampilan awal dari aplikasi *Wireshark* serupa dengan gambar yang ditampilkan dibawah ini.



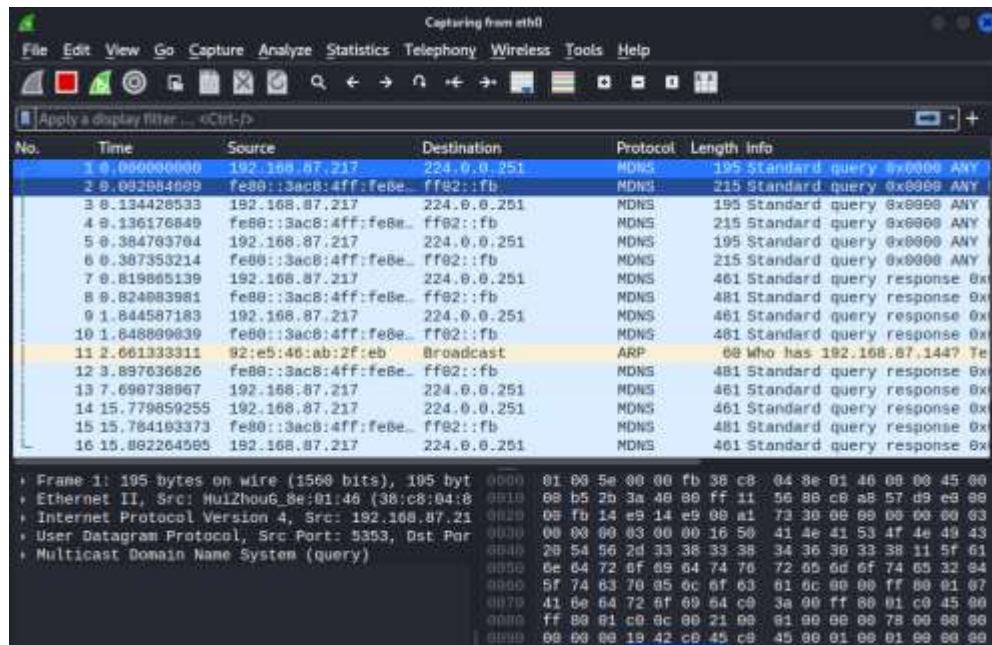
Gambar 4. 10 Tampilan awal *Wireshark*

12. Selanjutnya, memasuki antarmuka yang menampilkan paket data dalam jaringan, yang ditampilkan dalam bentuk diagram gelombang. Untuk masuk ke antarmuka Wi-Fi, penulis akan mengklik dua kali antarmuka tersebut..



Gambar 4. 11 Proses *Scanning* Jaringan

13. Setelah berhasil masuk ke dalam *interface*, aplikasi Wireshark akan secara otomatis memulai proses pengambilan data yang melalui jaringan Wi-Fi.

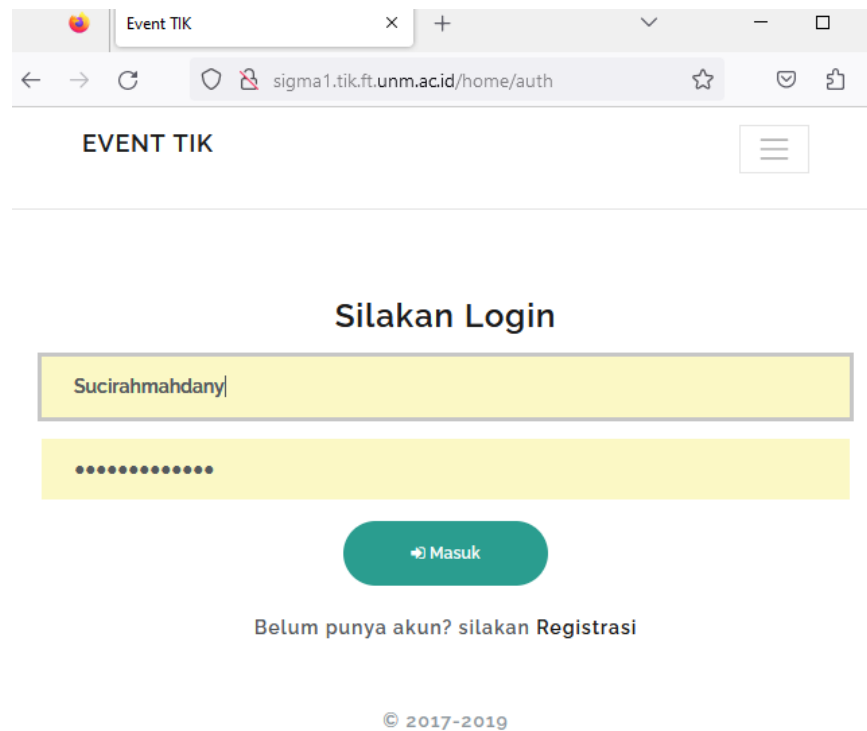


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.87.217	224.0.0.251	MDNS	195	Standard query 0x0000 ANY
2	0.002084009	fe80::3ac8:4ff:fe8e...	ff02::fb	MDNS	215	Standard query 0x0000 ANY
3	0.134428533	192.168.87.217	224.0.0.251	MDNS	195	Standard query 0x0000 ANY
4	0.136176849	fe80::3ac8:4ff:fe8e...	ff02::fb	MDNS	215	Standard query 0x0000 ANY
5	0.384763704	192.168.87.217	224.0.0.251	MDNS	195	Standard query 0x0000 ANY
6	0.387353214	fe80::3ac8:4ff:fe8e...	ff02::fb	MDNS	215	Standard query 0x0000 ANY
7	0.819885139	192.168.87.217	224.0.0.251	MDNS	461	Standard query response 0x...
8	0.824083981	fe80::3ac8:4ff:fe8e...	ff02::fb	MDNS	481	Standard query response 0x...
9	1.844587183	192.168.87.217	224.0.0.251	MDNS	461	Standard query response 0x...
10	1.848890039	fe80::3ac8:4ff:fe8e...	ff02::fb	MDNS	481	Standard query response 0x...
11	2.661333311	02:eb:46:ab:2f:eb	Broadcast	ARP	68	Who has 192.168.87.144? Te...
12	3.897336826	fe80::3ac8:4ff:fe8e...	ff02::fb	MDNS	481	Standard query response 0x...
13	7.690738067	192.168.87.217	224.0.0.251	MDNS	461	Standard query response 0x...
14	15.779859255	192.168.87.217	224.0.0.251	MDNS	461	Standard query response 0x...
15	15.764183373	fe80::3ac8:4ff:fe8e...	ff02::fb	MDNS	481	Standard query response 0x...
16	15.862264505	192.168.87.217	224.0.0.251	MDNS	461	Standard query response 0x...

Frame 1: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface eth0
 Ethernet II, Src: HuiZhouG_8e:01:46 (38:c8:04:8e:01:46), Dst: 01:00:5e:00:00:fb (01:00:5e:00:00:fb)
 Internet Protocol Version 4, Src: 192.168.87.217, Dst: 224.0.0.251
 User Datagram Protocol, Src Port: 5353, Dst Port: 5353
 Multicast Domain Name System (query)

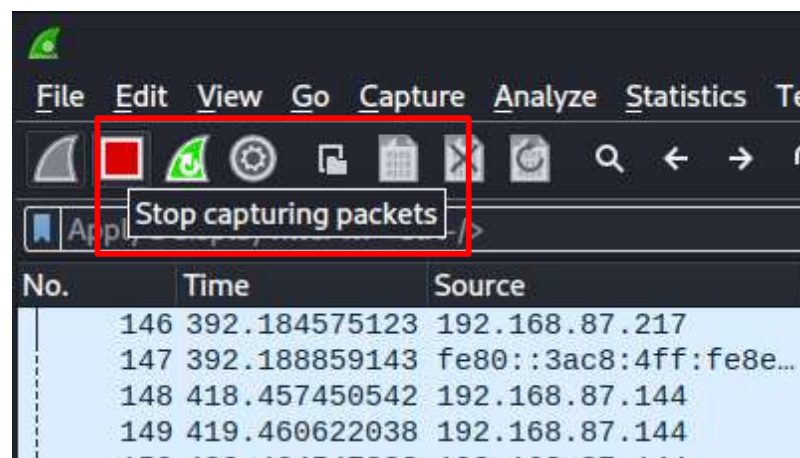
Gambar 4. 12 Paket Data Target

14. Memasuki tahapan pengujian keamanan, penulis mencoba mengakses *website-website* yang sering digunakan di Jurusan Teknik Informatika dan Komputer UNM diantaranya *website* SIMPEL, SIM-TA, IDS, Sigmatik, dan SIPI. Selanjutnya, penulis melakukan proses *login* pada laptop korban melalui aplikasi *Google*. Perangkat ini terkoneksi ke jaringan Wi-Fi yang sama dengan yang digunakan oleh penyerang.



Gambar 4. 13 Proses *Login* pada *Website*

15. Tunggu beberapa saat sampai semua data dari *website-website* tersebut tertangkap. Setelah itu, hentikan proses pemantauan dalam aplikasi Wireshark dengan cara klik “*Stop packet capture*” yang terletak dimenu bar seperti Gambar 4.14 *Stop Capture* dibawah ini.



Gambar 4. 14 *Stop Capture*

Dalam penelitian ini, peneliti menggunakan dua *hotspot* sebagai parameter serta empat akun dan perangkat sebagai target untuk memperoleh hasil penelitian yang lebih valid. Oleh karena itu, hasil penelitian direalisasikan ke dalam Tabel 4.

1 Hasil Penelitian Menggunakan *Hotspot* Broadband_UNM dan Tabel 4. 2 Hasil Penelitian Menggunakan *Hotspot* Pribadi berikut.

Tabel 4. 1 Hasil Penelitian Menggunakan *Hotspot* Broadband_UNM

Situs web yang diuji	Akun (target)	Hasil Penelitian	Keterangan
SIMPEL	User 1 (192.168.1.47)	Terenkripsi	Aman
	User 2 (192.168.1.74)	Terenkripsi	
	User 3 (192.168.1.27)	Terenkripsi	
	User 4 (192.168.1.63)	Terenkripsi	
IDS	User 1 (192.168.1.47)	Terenkripsi	Aman
	User 2 (192.168.1.74)	Terenkripsi	
	User 3 (192.168.1.27)	Terenkripsi	
	User 4 (192.168.1.63)	Terenkripsi	
SIM-TA	User 1 (192.168.1.47)	Terenkripsi	Aman
	User 2 (192.168.1.74)	Terenkripsi	
	User 3 (192.168.1.27)	Terenkripsi	
	User 4 (192.168.1.63)	Terenkripsi	
Sigmatik	User 1 (192.168.1.47)	<i>Username, dan password</i>	Rentan Terhadap Serangan <i>Packet Snifing</i>
	User 2 (192.168.1.74)	<i>Username, dan password</i>	
	User 3 (192.168.1.27)	<i>Username, dan password</i>	
	User 4 (192.168.1.63)	<i>Username, dan password</i>	
SIPI	User 1 (192.168.1.47)	<i>Username, dan password</i>	Rentan Terhadap Serangan <i>Snifing</i>
	User 2 (192.168.1.74)	<i>Username, dan password</i>	
	User 3 (192.168.1.27)	<i>Username, dan password</i>	
	User 4 (192.168.1.63)	<i>Username, dan password</i>	

Tabel 4. 2 Hasil Penelitian Menggunakan *Hotspot* Pribadi

Situs web yang diuji	Akun (target)	Hasil Penelitian	Keterangan
SIMPEL	User 1 (192.168.45.207)	Terenkripsi	Aman
	User 2 (192.168.255.15)	Terenkripsi	
	User 3 (192.168.195.189)	Terenkripsi	
	User 4 (192.168.43.220)	Terenkripsi	
IDS	User 1 (192.168.45.207)	Terenkripsi	Aman
	User 2 (192.168.255.15)	Terenkripsi	
	User 3 (192.168.195.189)	Terenkripsi	
	User 4 (192.168.43.220)	Terenkripsi	
SIM-TA	User 1 (192.168.45.207)	Terenkripsi	Aman
	User 2 (192.168.255.15)	Terenkripsi	
	User 3 (192.168.195.189)	Terenkripsi	
	User 4 (192.168.43.220)	Terenkripsi	
Sigmatik	User 1 (192.168.45.207)	<i>Username, dan password</i>	Rentan Terhadap Serangan <i>Packet Snifing</i>
	User 2 (192.168.255.15)	<i>Username, dan password</i>	
	User 3 (192.168.195.189)	<i>Username, dan password</i>	
	User 4 (192.168.43.220)	<i>Username, dan password</i>	
SIPI	User 1 (192.168.45.207)	<i>Username, dan password</i>	Rentan Terhadap Serangan <i>Snifing</i>
	User 2 (192.168.255.15)	<i>Username, dan password</i>	
	User 3 (192.168.195.189)	<i>Username, dan password</i>	
	User 4 (192.168.43.220)	<i>Username, dan password</i>	

Pada Tabel 4.1 Hasil Penelitian Menggunakan *Hotspot* Broadband_UNM adalah hasil uji coba serangan *packet sniffing* menggunakan *hotspot* yang digunakan secara umum di Jurusan Teknik Informatika dan Komputer yang dilindungi oleh keamanan Wi-Fi *protected access -pre shared key* (WPA2-Personal). Sehingga pengguna yang mengetahui *password hotspot* tersebut dapat terhubung. Dengan bantuan aplikasi *Etercap* dapat menampilkan perangkat atau *User* yang sedang terhubung dengan *hotspot* Broadband_UNM, dimana dengan adanya aplikasi ini peneliti dapat menentukan target perangkat yang akan diserang. Untuk itu, peneliti melakukan beberapa skenario uji coba pada *website* dengan menggunakan perangkat yang berbeda-beda.

Pada skenario uji coba menggunakan *hotspot* pribadi yang dilindungi oleh keamanan Wi-Fi *protected access -pre shared key* (WPA2-Personal) dimana hasil uji coba serangan ditampilkan pada Tabel 4.2 Hasil Penelitian Menggunakan *Hotspot* Pribadi, teridentifikasi hanya sedikit yang terkoneksi dalam jaringan. Sehingga, tidak semua orang dapat terhubung dalam *hotspot* tersebut. Meskipun demikian, pengujian serangan *sniffing* baik menggunakan *hotspot* Broadband_UNM atau *hotspot* pribadi, tetap menunjukkan bahwa beberapa *website* masih memiliki kerentanan terhadap jenis serangan ini. Namun, menggunakan *hotspot* Broadband_UNM menjadi peluang besar bagi *attacker* untuk melakukan serangan *sniffing* karena banyak teridentifikasi alamat IP, dan MAC *address* target pada aplikasi *Etercap*.

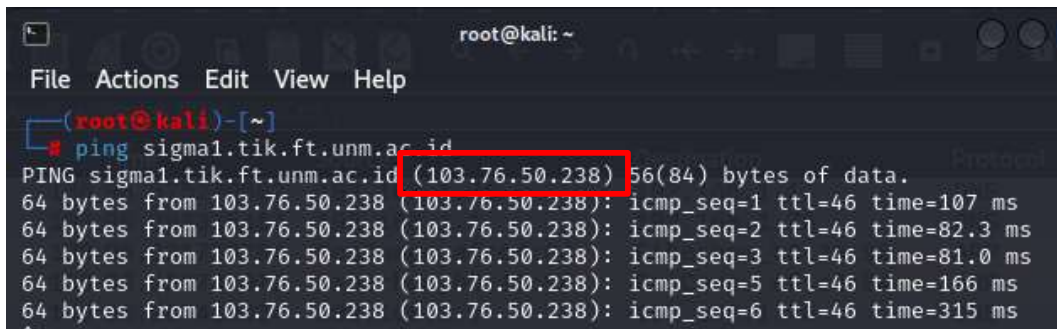
No.	Time	Source	Destination	Protocol	Length	Info
136	96.875278802	192.168.1.76	192.168.1.1	DNS	83	Standard query 0x4e43
137	96.883325464	192.168.1.1	192.168.1.76	DNS	99	Standard query response
138	96.931776794	PcsCompu_af:c4:84	Fiberhom_b3:10:98	ARP	42	who has 192.168.1.1? T
139	96.956741071	Fiberhom_b3:10:98	PcsCompu_af:c4:84	ARP	60	192.168.1.1 is at 0c:8
140	96.987410034	192.168.1.1	192.168.1.76	DNS	144	Standard query response
141	96.988195361	192.168.1.76	103.76.50.238	ICMP	98	Echo (ping) request 1
142	96.998841501	103.76.50.238	192.168.1.76	ICMP	98	Echo (ping) reply 1
143	96.999617291	192.168.1.76	192.168.1.1	DNS	86	Standard query 0x2ddf
144	97.021250003	62:32:b1:09:04:1d	Broadcast	ARP	60	who has 192.168.1.37? T
145	97.040463619	62:32:b1:09:04:1d	Broadcast	ARP	60	who has 192.168.1.27? T
146	97.040832681	62:32:b1:09:04:1d	Broadcast	ARP	60	who has 192.168.1.76? T
147	97.040847422	PcsCompu_af:c4:84	62:32:b1:09:04:1d	ARP	42	192.168.1.76 is at 08:
148	97.087089488	192.168.1.1	192.168.1.76	DNS	198	Standard query response
149	97.431748854	Fiberhom_b3:10:98	Broadcast	ARP	60	who has 192.168.1.47? T
150	97.999186363	192.168.1.76	103.76.50.238	ICMP	98	Echo (ping) request 1
151	97.999434223	103.76.50.238	192.168.1.76	ICMP	98	Echo (ping) reply 1

* Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 * Ethernet II, Src: 62:32:b1:09:04:1d (62:32:b1:09:04:1d), Dst: 01:00:00:00:00:00
 * Address Resolution Protocol (request)
 0820 00 00 00 00 00 00 c0 a8 01 1a 00 00 00 00 00 00
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Gambar 4. 15 *Capture Packet Sniffing* pada Wireshark

Pada Gambar 4.15 *Capture Packet Sniffing* pada Wireshark menampilkan hasil perekaman serangan *packet sniffing* yang terekam oleh aplikasi Wireshark, yang mencatat semua aktifitas yang ada dalam jaringan.

Untuk memeriksa paket yang berasal dari *website* SIMPEL, SIM-TA, IDS, Sigmatik, dan SIPI, diperlukan langkah penyaringan (*filtering*) dari data yang sudah tercatat. Sebelum menerapkan *filtering*, peneliti perlu mengetahui alamat IP dari ke-5 *website* tersebut yang diperoleh dari DNS pada *website*. Ini bisa dilakukan dengan melakukan langkah-langkah berikut, membuka terminal dan memasukkan perintah “#ping (nama DNS *website*)”, sebagai contoh “#ping sigma1.jtik.ft.unm.ac.id”, kemudian klik “Enter” di-keyboard, dan alamat IP dari sigma1.tik.ft.unm.ac.id akan muncul seperti pada Gambar 4.16 IP Address Website Sigmatik berikut.



```

root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# ping sigma1.tik.ft.unm.ac.id
PING sigma1.tik.ft.unm.ac.id (103.76.50.238) 56(84) bytes of data:
64 bytes from 103.76.50.238 (103.76.50.238): icmp_seq=1 ttl=46 time=107 ms
64 bytes from 103.76.50.238 (103.76.50.238): icmp_seq=2 ttl=46 time=82.3 ms
64 bytes from 103.76.50.238 (103.76.50.238): icmp_seq=3 ttl=46 time=81.0 ms
64 bytes from 103.76.50.238 (103.76.50.238): icmp_seq=5 ttl=46 time=166 ms
64 bytes from 103.76.50.238 (103.76.50.238): icmp_seq=6 ttl=46 time=315 ms

```

Gambar 4. 16 IP Address Website Sigmatik

Tabel 4. 3 IP Address Website JTIK

Website	DNS (Domain Name System)	IP Address
SIMPEL	simpel.jtik.ft.unm.ac.id	103.76.50.235
SIM-TA	simta.jtik.ft.unm.ac.id	103.76.50.235
IDS	ids.tik.ft.unm.ac.id	103.76.50.235
Sigmatik	sigma1.tik.ft.unm.ac.id	103.76.50.238
SIPI	Sipi.jtik.ft.unm.ac.id	103.76.50.235

Pada Gambar 4.16 IP Address Sigmatik, menampilkan angka yang dilingkari dengan persegi panjang berwarna merah adalah IP address dari website Sigmatik, dan untuk lebih jelasnya dipaparkan pada Tabel 4.3. IP Address Website JTIK. Setelah mengetahui bahwa IP address dari website-website tersebut, Tahap selanjutnya adalah melakukan penyaringan paket berdasarkan IP Address menggunakan bilah filter yang terdapat di bawah ikon aplikasi Wireshark. Ini dapat dilakukan dengan memasukkan perintah "ip.addr==(IP Address website)". Sebagai contoh untuk website Sigmatik "ip.addr==103.76.50.238", akan menghasilkan tampilan paket-paket yang berkaitan dengan alamat IP tersebut.

No.	Time	Source	Destination	Protocol	Length	Info
1376	485.435217364	103.76.50.238	192.168.1.47	TCP	60	88 → 62780 [SYN, ACK] Seq=6 Ack=1 Win=
1377	485.435217640	192.168.1.47	103.76.50.238	TCP	60	62781 → 88 [SYN] Seq=0 Win=64240 Len=
1378	485.439604438	103.76.50.238	192.168.1.47	TCP	60	[TCP Retransmission] 88 → 62780 [SYN
1379	485.439130006	192.168.1.47	103.76.50.238	TCP	60	[TCP Retransmission] [TCP Port number
1380	485.465351944	103.76.50.238	192.168.1.47	TCP	60	88 → 62781 [SYN, ACK] Seq=6 Ack=1 Win=
1381	485.471229372	103.76.50.238	192.168.1.47	TCP	60	[TCP Retransmission] 88 → 62781 [SYN
1382	485.500533735	192.168.1.47	103.76.50.238	TCP	60	62780 → 88 [ACK] Seq=1 Ack=1 Win=6424
1383	485.501894875	192.168.1.47	103.76.50.238	HTTP	803	GET /home/auth HTTP/1.1
1384	485.503137886	192.168.1.47	103.76.50.238	TCP	54	62780 → 88 [ACK] Seq=1 Ack=1 Win=6424
1385	485.503290178	192.168.1.47	103.76.50.238	TCP	60	[TCP Retransmission] 62780 → 88 [PSH
1386	485.526944961	192.168.1.47	103.76.50.238	TCP	60	62781 → 88 [ACK] Seq=1 Ack=1 Win=6424
1387	485.527277824	192.168.1.47	103.76.50.238	TCP	54	[TCP Dup ACK 1386x1] 62781 → 88 [ACK
1388	485.630316307	103.76.50.238	192.168.1.47	TCP	60	[TCP window update] 88 → 62780 [ACK]
1389	485.630316953	103.76.50.238	192.168.1.47	TCP	60	[TCP window update] 88 → 62781 [ACK]
1390	485.630311063	103.76.50.238	192.168.1.47	TCP	60	88 → 62780 [ACK] Seq=1 Ack=800 Win=3
1391	485.630311356	103.76.50.238	192.168.1.47	TCP	60	[TCP Dup ACK 1390x1] 88 → 62780 [ACK

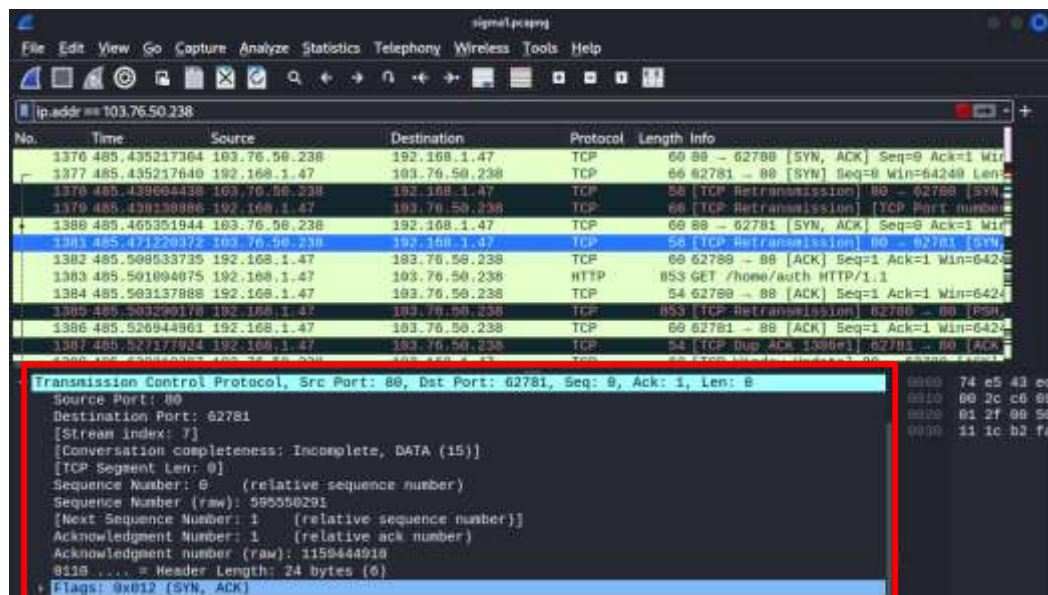
Gambar 4. 17 Paket data dari website Sigmatik

Pada Gambar 4.17 Paket data dari website Sigmatik, menampilkan semua paket data yang berkaitan dengan IP address 103.76.50.238 entah itu yang berasal dari sumber (*Source*) atau pada ditujukan ke tujuan (*Destination*).

Terlihat bahwa posisi *Source* dan *Destination* selalu berganti tempat. Dalam semua data yang terlihat, ada dua tipe protokol yang digunakan, yakni protokol *Transmission Control Protocol* (TCP) dan protokol *Hypertext Transfer Protocol* (HTTP). Dikarenakan mayoritas hubungan internet menggunakan protokol TCP, maka paket-paket TCP yang direkam menjadi sangat dominan.

Dapat diamati juga tampilan visual paket data, beberapa paket menampilkan warna hijau muda, mengindikasikan penggunaan protokol HTTP dan TCP melalui port 80. Sementara itu, paket yang ditandai dengan warna hitam dan tulisan merah menandakan bahwa paket tersebut bermasalah dan perlu dilakukan pengiriman ulang paket data.

Untuk melakukan analisis paket data, informasi dapat ditemukan dalam panel rincian *packet* data. Berikut ini adalah contoh tampilan detail *packet* data untuk protokol TCP.



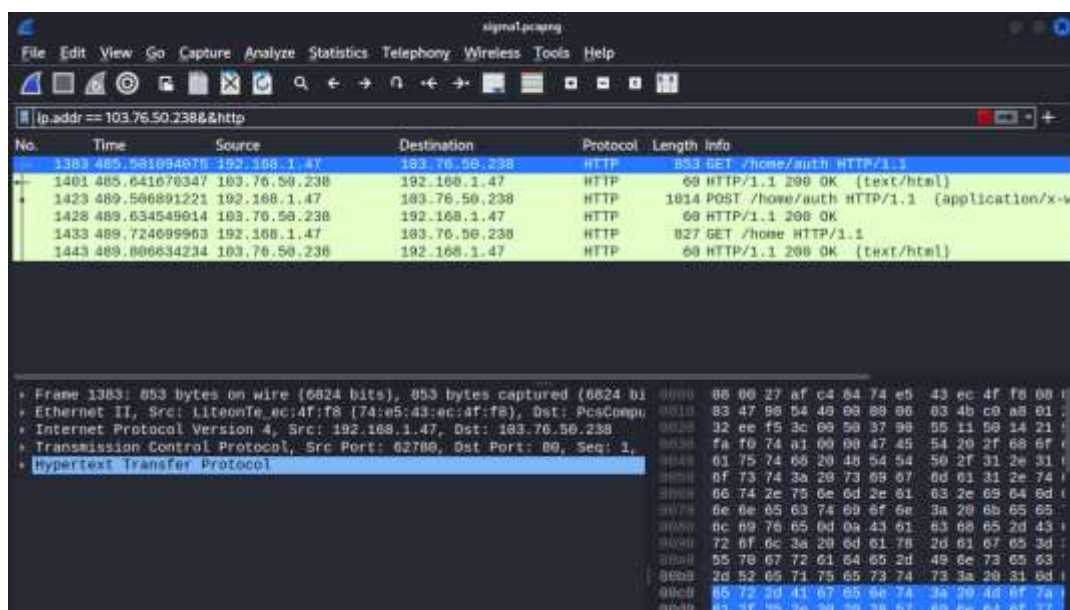
Gambar 4. 18 Rincian *Packet* TCP

Pada Gambar 4.18 menampilkan rincian dari *packet* *Transmission Control Protocol* yang telah diberi tanda persegi panjang berwarna merah. Dari rincian paket data tersebut, penulis dapat menganalisis informasi sebagai berikut:

Tabel 4. 4 Analisis Rincian *packet* data

Informasi	Hasil Analisis	Keterangan
Source Port	62781	Menunjukkan bahwa <i>client</i> menggunakan <i>port</i> 62781.
Destination Port	HTTP (80)	Menunjukkan bahwa <i>port</i> yang digunakan server adalah 80 yaitu http.
Flags	0x002 (SYN)	Menunjukkan bahwa <i>client</i> ingin mengambil data dari server.

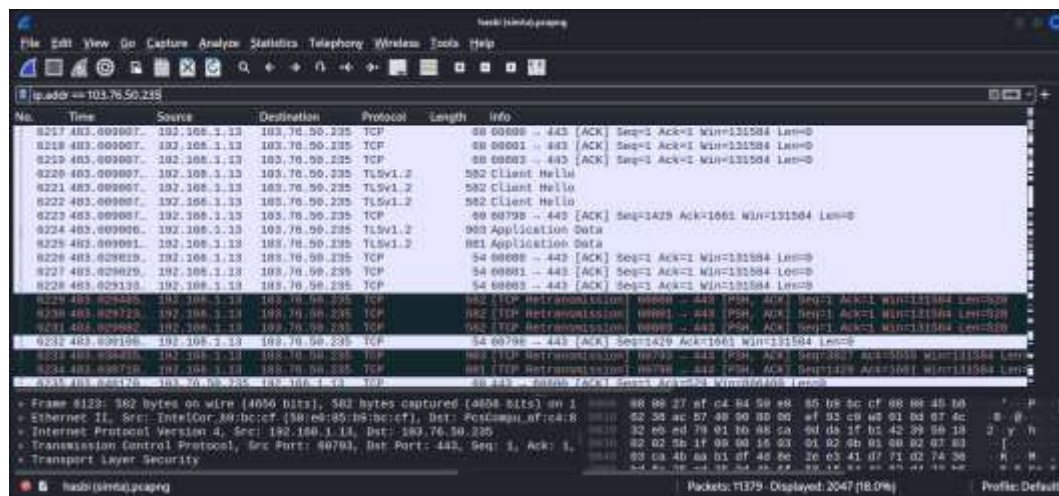
Dikarenakan penelitian ini berfokus pada analisis keamanan *website*, penulis akan melakukan *filtering* tambahan menggunakan perintah “ip.addr==103.76.50.238&&http” untuk *website* Sigmatik dan “ip.addr==103.76.50.238&&http” untuk *website* SIPI, yang akan menampilkan paket-paket dengan protokol HTTP, seperti yang terlihat dalam Gambar 4.19 *Filtering* Protokol HTTP dibawah ini.



Gambar 4. 19 *Filtering* Protokol HTTP

Dalam konteks ini, data yang berasal dari *website* Sigmatik melalui protokol HTTP ditampilkan. Setelah proses *filtering* protokol HTTP, terdapat 6 paket data yang tersisa pada Gambar 4.19 *Filtering* Protokol HTTP. Didalam menu “Info” terdapat beberapa informasi seperti GET, HTTP/1.1, dan POST.

Ditemukan perbedaan yang signifikan dari *website* yang menggunakan lapisan keamanan SSL/TLS seperti pada *website* SIMPEL, SIM-TA, dan IDS.

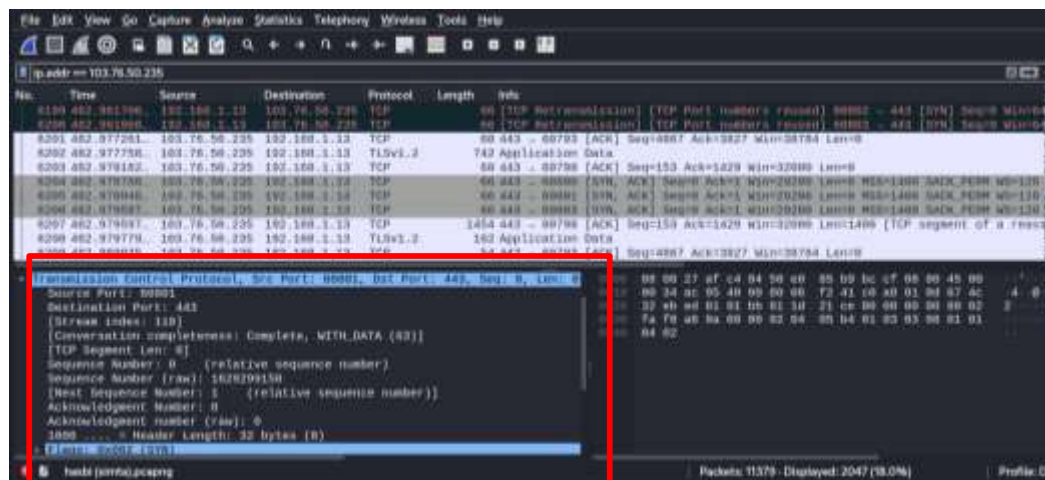


Gambar 4. 20 Paket data *Website* SIMPEL yang Terekam

Pada Gambar 4.20 Paket Data *Website* SIMPEL yang Terekam, menampilkan semua paket data dari *website* yang mempunyai lapisan keamanan dimana terdapat dua tipe protokol yang digunakan, yakni protokol *Transmission Control Protocol* (TCP) dan protokol *Transport Layer Security* (TLS).

Dapat diamati juga tampilan visual dari Gambar 4.20 Paket Data *Website* SIMPEL yang terekam, sejumlah paket menggunakan warna abu-abu muda, yang mengindikasikan penggunaan protokol TLS dan protokol TCP melalui *port* 443. Paket yang berwarna abu-abu gelap menandakan keberadaan *flag* SYN dan FIN, atau keduanya. Sementara itu, paket yang ditandai dengan warna hitam dan teks merah menunjukkan adanya masalah dan perlu dilakukan pengiriman ulang paket data.

Untuk melakukan analisis paket data, informasi dapat ditemukan dalam panel rincian paket data. Gambar 4. 21 Rincian *Packet Data* TCP ini menampilkan rincian paket data data untuk protokol TCP.

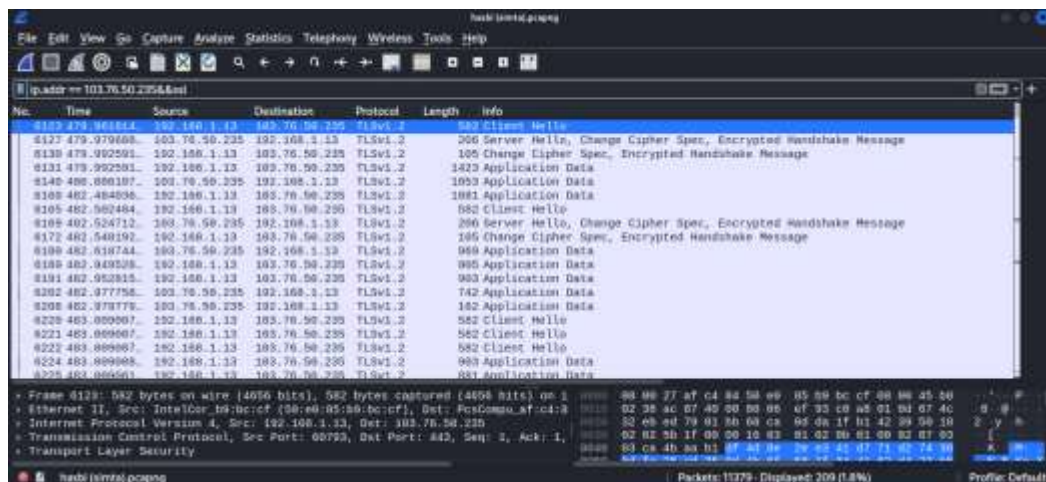
Gambar 4. 21 Rincian *Packet Data TCP*

Pada Gambar 4.21 Rincian *Packet Data TCP* menampilkan rincian dari *packet Transmission Control Protocol* yang telah diberi kotak merah. Dari rincian paket data tersebut, penulis dapat melakukan analisis terhadap informasi yang disajikan dalam Tabel 4.5 Analisis Rincian *Packet Data HTTPS* berikut:

Tabel 4. 5 Analisis Rincian *Packet Data HTTPS*

Informasi	Hasil Analisis	Keterangan
<i>Source Port</i>	60801	Menunjukkan bahwa <i>client</i> menggunakan <i>port</i> 60801.
<i>Destination Port</i>	HTTPS (443)	Menunjukkan bahwa <i>port</i> yang digunakan server adalah 443 yaitu HTTPS.
<i>Flags</i>	0x002 (SYN)	Menunjukkan bahwa <i>client</i> ingin mengambil data dari server.

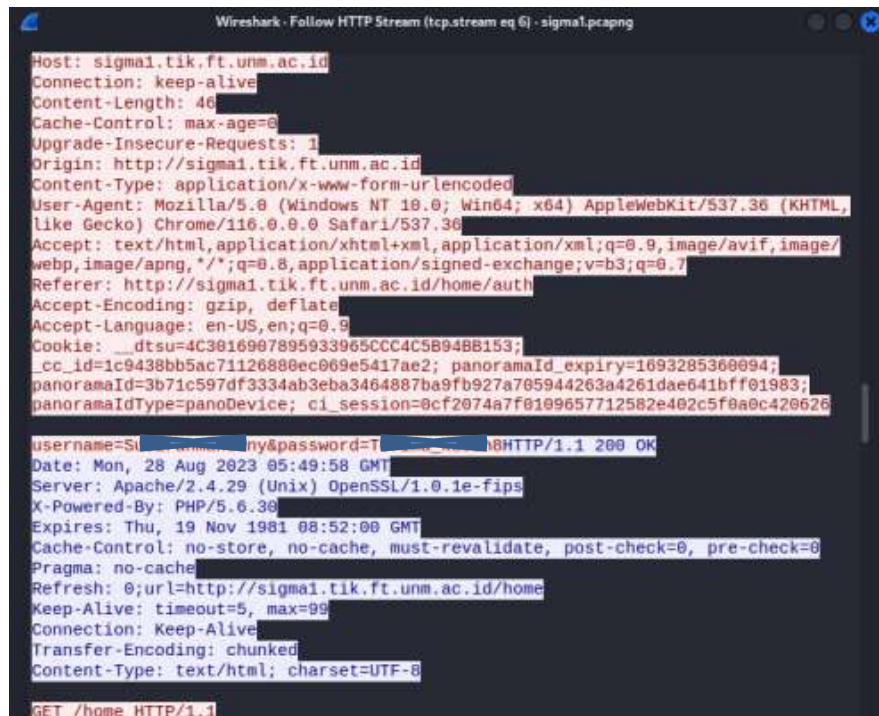
Seperti halnya dengan *website* yang memiliki protokol HTTP, maka penulis melakukan *filtering* tambahan dengan memasukkan perintah “ip.addr==103.76.50.235&&ssl”, yang akan menampilkan paket-paket dengan protokol TLS, seperti yang tampak dalam Gambar 4.22 Daftar Paket *Website SIM-TA* dibawah ini.



Gambar 4. 22 Daftar paket *Website* SIM-TA

Dalam Gambar 4. 22 Daftar Paket *Website* SIM-TA, menunjukkan paket data yang berasal dari *website* SIM-TA dengan menggunakan protokol TLS. Didalam menu “Info”, terdapat beberapa informasi seperti *Client Hello*, *Server Hello*, *Certificate*, *Server Key Exchange*, *Encrypted Handshake Message*, *Client Key Exchange*, *Change Cipher Spec*, *New Session Ticket*, dan *Application Data*.

Untuk melakukan analisis pada paket data yang menggunakan protokol HTTP seperti *website* Sigmatik dan SIPI, dapat dilakukan dengan meng-klik kanan paket data pada *listing packet panel* yang ingin dianalisis, setelah itu pilih “*Follow HTTP Stream*”. Dalam Gambar 4. 23 Isi *Packet Follow HTTP Stream website* Sigmatik dan Gambar 4. 24 Isi *Packet Follow HTTP Stream Website* SIPI, ditampilkan rincian paket data protokol HTTP yang membawa informasi “POST”.



```

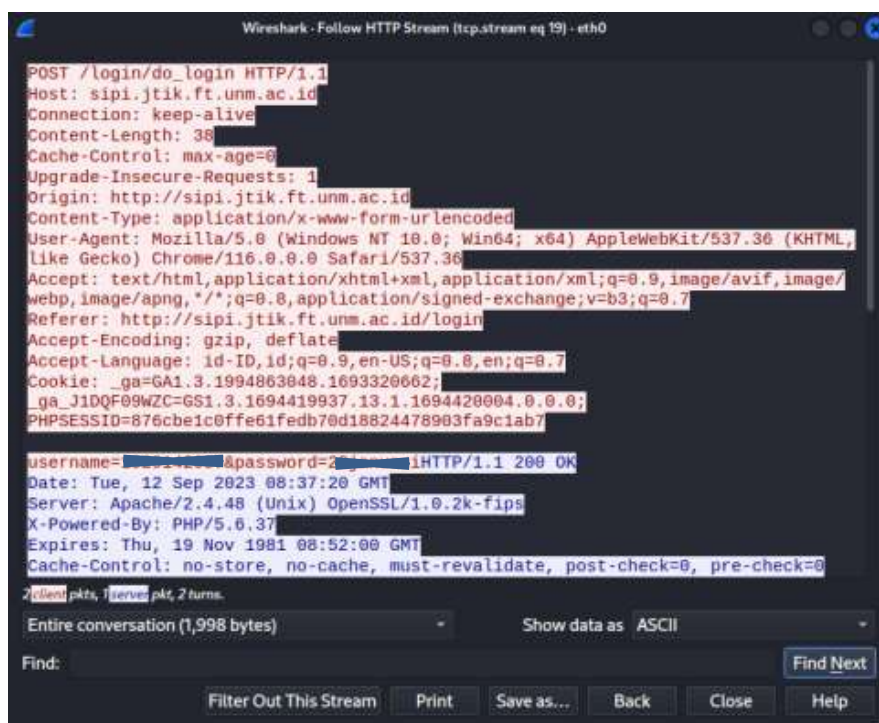
Host: sigma1.tik.ft.unm.ac.id
Connection: keep-alive
Content-Length: 40
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://sigma1.tik.ft.unm.ac.id
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 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://sigma1.tik.ft.unm.ac.id/home/auth
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __dtsu=4C3016907895933965CCC4C5B948B153; __cc_id=1c9438bb5ac71126880ec069e5417ae2; panoramaId_expiry=1693285360094; panoramaId=3b71c597df3334ab3eba3464887ba9fb927a705944263a4261dae641bff01983; panoramaIdType=panoDevice; ci_session=0cf2074a7f0109657712582e402c5f0a0c420626

username=Sigma1Tik&password=1234567890HTTP/1.1 200 OK
Date: Mon, 28 Aug 2023 05:49:58 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Refresh: 0;url=http://sigma1.tik.ft.unm.ac.id/home
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

GET /home HTTP/1.1

```

Gambar 4. 23 Isi Packet Follow HTTP Stream Website Sigmatik



```

POST /login/do_login HTTP/1.1
Host: sipi.jtik.ft.unm.ac.id
Connection: keep-alive
Content-Length: 38
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://sipi.jtik.ft.unm.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/116.0.0.0 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://sipi.jtik.ft.unm.ac.id/login
Accept-Encoding: gzip, deflate
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: __ga=GA1.3.1994863048.1693320662; __ga_j1DQF09WZC=GS1.3.1694419937.13.1.1694420004.0.0.0; PHPSESSID=876cbe1c0ffe61fedb70d18824478903fa9c1ab7

username=Sigma1Tik&password=1234567890HTTP/1.1 200 OK
Date: Tue, 12 Sep 2023 08:37:20 GMT
Server: Apache/2.4.48 (Unix) OpenSSL/1.0.2k-fips
X-Powered-By: PHP/5.6.37
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

2 client pkts, 1 server pkt, 2 turns.
Entire conversation (1,998 bytes)
Show data as ASCII
Find:
Filter Out This Stream Print Save as... Back Close Help

```

Gambar 4. 24 Isi Packet Follow HTTP Stream Website SIPI

Dari Gambar 4. 23 *Isi Packet Follow HTTP Stream website Sigmatik* dan Gambar 4. 24 *Isi Packet Follow HTTP Stream Website SIPI*, menampilkan bahwa dalam rincian paket data protokol HTTP terdapat dua jenis warna teks yang berbeda. Teks dengan warna merah menunjukkan adanya permintaan HTTP (*HTTP request*), sementara teks yang berwarna biru menunjukkan tanggapan HTTP (*HTTP response*).

Konten dari paket data yang berlabel "POST" berisi berbagai jenis informasi, termasuk data rahasia seperti *Username dan password*. Selain itu, dalam rincian paket data tersebut, peneliti dapat menganalisis beberapa informasi seperti pada Tabel 4. 6 Hasil Identifikasi paket data *Website Sigmatik*, dan Tabel 4.7 Hasil Identifikasi paket data *Website SIPI* berikut.

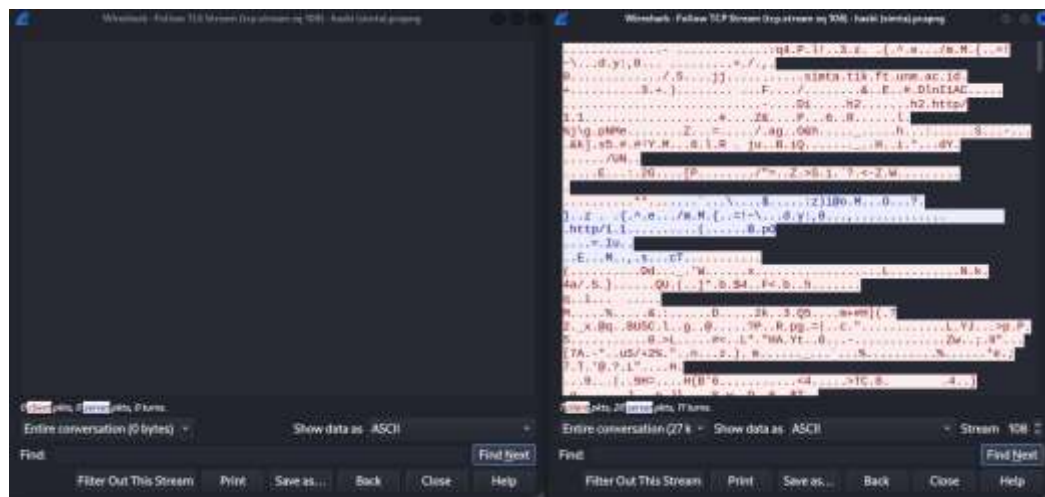
Tabel 4. 6 Hasil Identifikasi Paket Data Website Sigmatik

Website	Informasi	Hasil Analisis	Keterangan
Sigmatik	POST	-	Memberitahukan bahwa <i>client</i> melakukan sebuah permintaan dengan menggunakan isi pesan untuk mengirim data ke <i>server web</i> .
	Host	sipi.jtik.ft.unm.ac.id	Menunjukkan bahwa <i>client</i> sedang terkoneksi dengan sipi.jtik.ft.unm.ac.id
	Connection	Keep-alive	Suatu parameter yang menentukan batas waktu maksimal saat koneksi terputus dan jumlah permintaan maksimum.
	Content-Type:	application/x-www-form-urlencoded; charset=UTF-8.	<i>Client</i> mengirimkan data melalui <i>Form Uniform Resource Locator</i> (URL)
	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, Like Gecko) Chrome/116.0.0.0 Safari/537.36.	Menyatakan kemungkinan <i>Web Browser</i> yang sedang digunakan oleh <i>client</i> .
	Accept-Encoding	gzip, deflate	Menunjukkan metode kompresi yang digunakan oleh <i>client</i> yaitu gzip atau deflate.
	Accept-Language	en-US, en ; q=0.9	Menunjukkan Bahasa yang diterima oleh server adalah Bahasa Inggris
	HTTP/1.1 200 OK.	-	Menyatakan permintaan telah berhasil dieksekusi.
	Date	Mon, 28 Aug 2023 05:49:58 GMT	Menunjukkan waktu ketika server mengirimkan data tersebut.
	Server	Apache	Jenis server yang digunakan yaitu <i>Apache</i> .

Tabel 4. 7 Hasil Identifikasi Paket Data Website SIPI

Website	Informasi	Hasil Analisis	Keterangan
SIPI	POST	-	Memberitahukan bahwa <i>client</i> melakukan sebuah permintaan dengan menggunakan isi pesan untuk mengirim data ke <i>server web</i> .
	<i>Host</i>	sigma1.tik.ft.unm.ac.id	Menunjukkan bahwa <i>client</i> sedang terkoneksi dengan sigma1.tik.ft.unm.ac.id
	<i>Connection</i>	<i>Keep-alive</i>	Suatu parameter yang menentukan batas waktu maksimal saat koneksi terputus dan jumlah permintaan maksimum.
	<i>Content-Type:</i>	application/x-www-form-urlencoded; charset=UTF-8.	<i>Client</i> mengirimkan data melalui <i>Form Uniform Resource Locator</i> (URL)
	<i>User-Agent:</i>	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, Like Gecko) Chrome/116.0.0.0 Safari/537.36.	Menyatakan kemungkinan <i>Web Browser</i> yang sedang digunakan oleh <i>client</i> .
	<i>Accept-Encoding</i>	gzip,deflate	Menunjukkan metode kompresi yang digunakan oleh <i>client</i> yaitu gzip atau deflate.
	<i>Accept-Language</i>	Id-ID, id;q=0.9,en-US;q=0.8, en;q=0.7	Menunjukkan Bahasa yang diterima oleh server adalah Bahasa Indonesia
	HTTP/1.1 200 OK.	-	Menyatakan permintaan telah berhasil dieksekusi.
	<i>Date</i>	Tue, 12 Sep 2023 08:37:20 GMT	Menunjukkan waktu ketika server mengirimkan data tersebut.
	Server	<i>Apache</i>	Jenis server yang digunakan yaitu <i>Apache</i> .

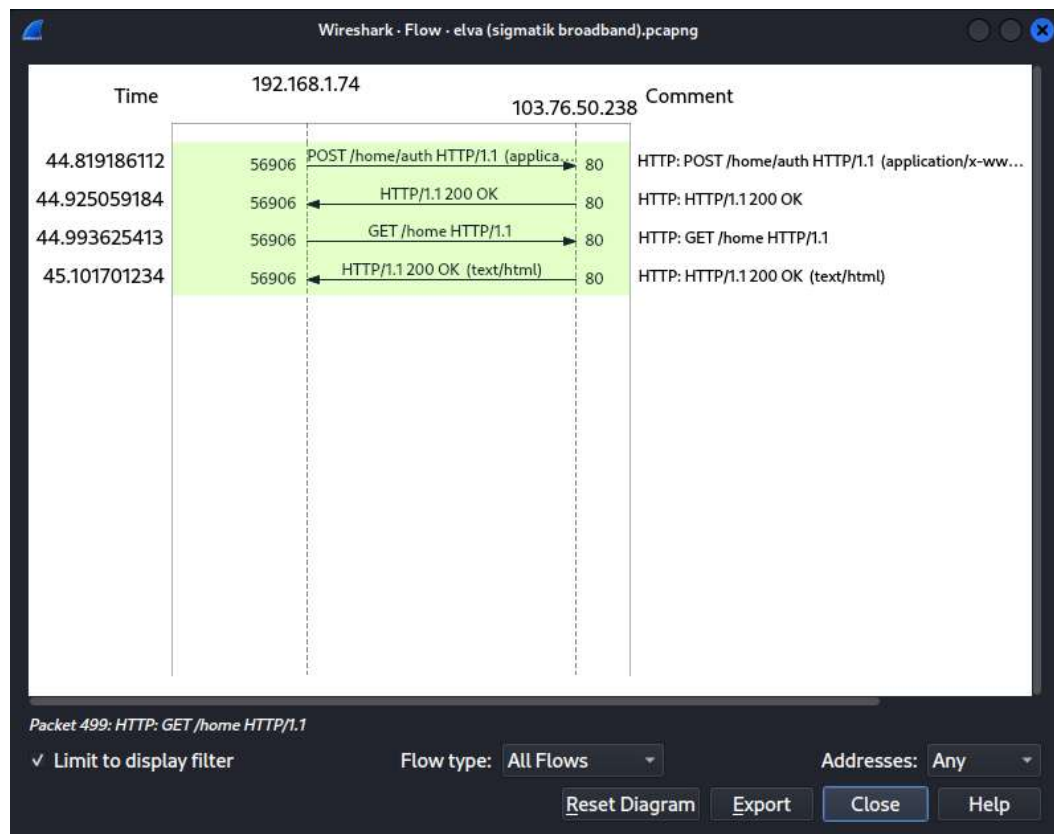
Sedangkan untuk melakukan analisis pada paket data yang memiliki lapisan keamanan seperti *website* SIMPEL, SIM-TA, dan IDS, dapat dilakukan dengan klik kanan paket data pada panel daftar paket yang ingin dianalisis, setelah itu pilih “*Follow TLS Stream*”. Gambar 4.25 Isi Paket Data *Follow TLS Stream* dan *TCP Stream Website SIM-TA* dibawah ini adalah contoh tampilan rincian paket data protokol TLS yang membawa informasi “*Application Data*”.



Gambar 4. 25 Isi Paket Data *Follow TLS Stream* dan *TCP Stream website SIM-TA*

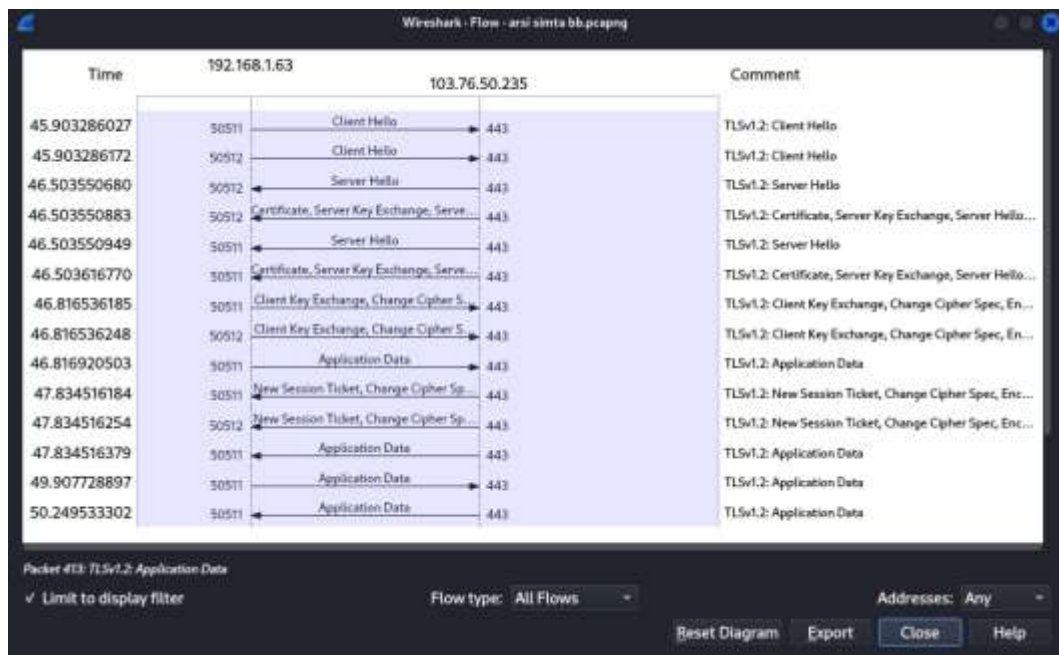
Dalam Gambar 4.25 Isi Paket Data *Follow TLS Stream* dan *TCP Stream Website SIM-TA*, menampilkan “*Follow TLS Stream*” dan “*Follow TCP Stream*” dari data yang telah dipilih. Dari rincian data protokol TLS tersebut, tidak ada informasi yang dapat ditemukan. Oleh karena itu, peneliti menganalisis paket data yang sama dengan cara mengklik kanan pada paket data yang akan dianalisis. dan memilih “*Follow TCP Stream*”. Namun, hasilnya peneliti tidak dapat dengan mudah menganalisis informasi karena yang dikirim telah melalui proses enkripsi.

Pemeriksaan proses komunikasi data yang terjadi ketika korban mengakses *website* Sigmatik dan SIPI, dengan mengklik “*Statistic*” di menu bar dan memilih “*Flow Graph*”.



Gambar 4. 26 Proses Komunikasi Data *Client* dan *Server* pada Protokol HTTP

Pada Gambar 4.26 Proses Komunikasi Data *Client* dan Server pada Protokol HTTP, menampilkan proses pertukaran data antara klien dengan *User 2* IP address 192.168.1.47 dan server yaitu sigma1.tik.ft.unm.ac.id dengan IP address 103.76.50.238.



Gambar 4. 27 Proses Komunikasi Data *Client* dan *Server* pada Protokol HTTPS

Pada Gambar 4.27 Proses Komunikasi Data *Client* dan *Server* pada Protokol HTTPS, menampilkan proses pertukaran data antara klien dengan *User* 4 IP address 192.168.1.63 dan server yaitu simta.tik.ft.unm.ac.id dengan IP address 103.76.50.235 dan melalui *gateway* 192.168.1.1.

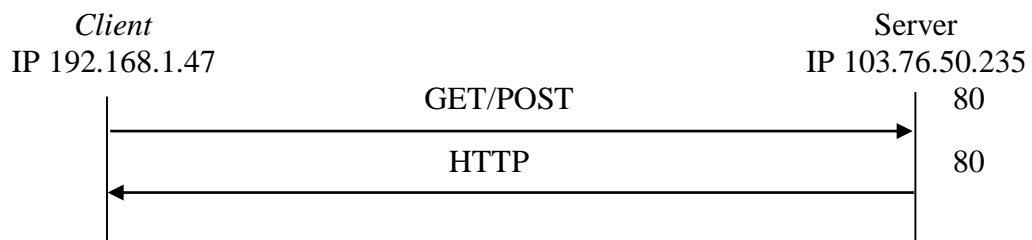
B. Pembahasan

Hasil dari pengujian serangan *packet sniffing* dalam penelitian ini mengindikasikan bahwa beberapa *website* di Jurusan Teknik Informatika dan Komputer UNM memiliki potensi kerentanan terhadap upaya pencurian data dengan menggunakan metode serangan *sniffing* pada jaringan nirkabel. Pada *website* SIMPEL, IDS, dan SIMTA dapat diklasifikasikan sebagai *website* yang aman, karena dalam pengujiannya dalam menyerang beberapa *User* dan perangkat, *website* tersebut tidak dapat ditemukan informasi apapun, selain informasi bahwa *website-website* tersebut terenkripsi. Berbeda halnya dengan *website* Sigmatik, dan

SIPI, peneliti dapat melihat data penting *User* seperti *Username* dan *password* pada saat melakukan aktivitas *login*. Hal tersebut disebabkan karena beberapa *website* seperti Sigmatik, dan SIPI masih menggunakan protokol HTTP, sedangkan *website* SIM-TA, SIMPEL, dan menggunakan protokol TLS atau HTTPS. Perbedaan utamanya terletak pada cara kerjanya.

Ketika target mengakses *website* Sigmatik, dan SIPI melalui *browser*, lalu *browser* akan meminta data dari server. Server kemudian mengirimkan data tersebut dalam format teks biasa melalui protokol TCP tanpa adanya lapisan keamanan tambahan. Akibatnya, ketika serangan *sniffing* dilakukan, semua data yang melalui komputer *attacker*, dapat terekam dalam aplikasi *Wireshark*, dan dari data itu juga dapat dengan mudah dipahami oleh *attacker*, seperti yang tampak pada Gambar 4. 23 Isi *Packet Follow HTTP Stream website* Sigmatik User1, dan Gambar 4. 24 Isi *Packet Follow HTTP Stream Website* SIPI

Dilihat dari Gambar 4.26 Proses Komunikasi Data *Client* dan Server pada Protokol HTTP, secara simpelnya, proses komunikasi data pada *website* yang menggunakan protokol HTTP seperti Sigmatik, dan SIPI dijelaskan dalam Gambar 4.28 Proses Komunikasi Data *Website* Sigmatik dan SIPI berikut.



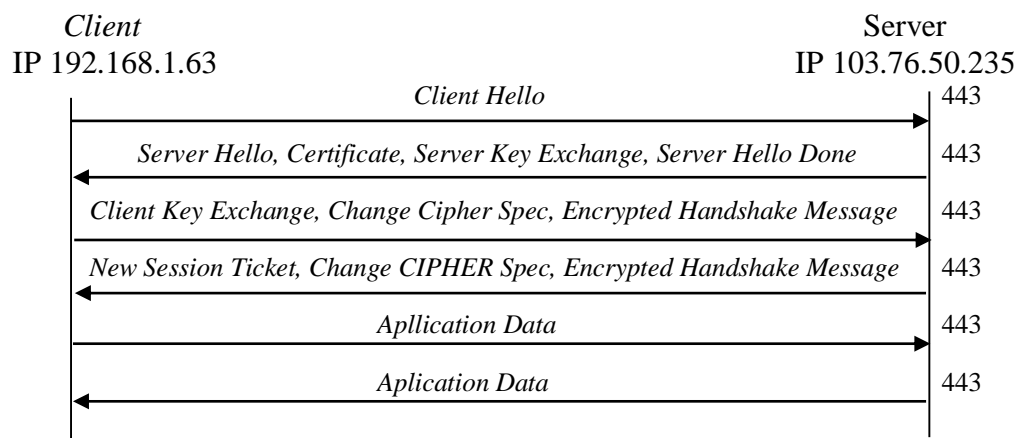
Gambar 4. 28 Proses Komunikasi Data *Website* Sigmatik dan SIPI

Dalam Gambar 4.28 Proses Komunikasi Data *Website* Sigmatik dan SIPI, Menggambarkan proses pertukaran data antara klien dan server *website* Sigmatik, dan SIPI secara sederhana. Terlihat bahwa ketika *client* meminta data dari *web server* terdapat dua pilihan yang tersedia yakni menggunakan metode GET atau menggunakan metode POST.

Pada saat *client* melakukan permintaan dengan menentukan parameter dibagian *Uniform Resource Locator* (URL), maka metode permintaan HTTP yang digunakan adalah GET. Contohnya adalah URL yang ada pada halaman web. Disisi lain, jika *client* melakukan permintaan dengan mengirimkan data ke server web melalui badan pesan, metode permintaan HTTP yang digunakan adalah POST. Contohnya adalah saat mengisi formulir *Username* dan *password* pada halaman web. Setelah itu, server akan mengirimkan respon HTTP ke *client* yang berisi data yang diminta dalam bentuk teks biasa.

Situasi berbeda terjadi pada *website* SIM-TA, SIMPEL, dan IDS. Ketika target mengakses *website* tersebut melalui *browser*, *browser* tersebut sebagai *client* akan meminta data dari server. Namun, server tidak mengirimkan data yang diminta secara langsung. Hal ini terjadi karena klien dan server akan melakukan komunikasi awal untuk memverifikasi identitasnya terlebih dahulu. Lalu dilakukan perundingan mengenai kode privasi sebelum komunikasi data dilakukan. Oleh karena itu, ketika proses dalam *sniffing* dilakukan, data yang melalui komputer *attacker* tidak dapat dengan mudah terbaca dalam aplikasi *Wireshark*, seperti yang tampak dalam Gambar 4. 25 Isi Paket Data *Follow TLS Stream* dan *TCP Stream Website SIM-TA*.

Dalam Gambar 4.27 Proses Komunikasi Data *Client* dan Server pada Protokol HTTPS, secara simpelnya, proses komunikasi data pada *website* yang menggunakan protokol HTTPS pada *website* SIM-TA, SIMPEL, dan IDS digambarkan seperti berikut.



Gambar 4. 29 Proses Komunikasi Data Protokol HTTPS Pada *Website* SIM-TA

Gambar 4.29 Proses Komunikasi Data Protokol HTTPS Pada *Website* SIM-TA, menggambarkan proses komunikasi yang sederhana antara *client* dengan server *website* SIM-TA. Pada gambar tersebut terlihat *Client* mengirimkan permintaan "*Client Hello*" kepada server. Kemudian, Server membalas dengan mengirimkan pesan "*Server Hello*" kepada client dan mengikutsertakan kunci publik server untuk melaksanakan pertukaran kunci publik dengan *client*. Selain itu, server juga mengirimkan sertifikatnya kepada *client* sebagai bagian dari proses otentikasi. Setelah itu, server membalas pesan dengan "*Server hello done*". Apabila sertifikat tersebut telah diterbitkan oleh salah satu otoritas sertifikasi atau CA (*Certification Authority*) yang terpercaya dan terdaftar dalam daftar CA yang diakui oleh *web browser*, maka *client* dapat menverifikasi *public key server*. Selanjutnya,

ketika *client* mengirimkan pemberitahuan "*Change Cipher Spec*" kepada server untuk menandakan bahwa *client* akan memulai penggunaan *public key* untuk melakukan enkripsi pesan. Setelah itu, server memulai sesi baru dengan mengirimkan notifikasi "*Change Cipher Spec*" ke *client* menunjukkan bahwa server akan memulai menggunakan tiket sesi yang mencakup semua pesan yang telah dibahas sebelumnya dan akan mengenkripsinya dengan *secret key* yang hanya diketahui oleh server. Selanjutnya, *client* dan server kemudian bisa bertukar data aplikasi melalui saluran yang aman yang telah dibuat oleh keduanya.

Setelah menyelesaikan transmisi data, jika *client* ingin meminta data tambahan dari server, *client* akan mengirim pesan "*Client Hello*" dengan menggunakan ID sesi dari sesi sebelumnya. Kemudian, server akan memeriksa *session cache* untuk mencocokkan ID sesi tersebut. Jika ada kesamaan yang ditemukan, server dapat melanjutkan sesi dan mengirim pesan "*Server Hello*". Setelah itu, *client* dan server akan melakukan pertukaran pesan "*Change Cipher Spec*". Dengan langkah-langkah ini, *client* dan server bisa mengirim data aplikasi melalui saluran yang aman yang telah ditetapkan sebelumnya.

a. Solusi Untuk Mencegah Serangan *Packet Sniffing*

Packet sniffing adalah ancaman serius yang dapat mengintai lalu lintas data di internet, mengancam privasi dan keamanan data pengguna. Dalam penelitian ini, penulis mengidentifikasi dua *website* yang rentan terhadap serangan sniffing, yaitu *website* Sigmatik, dan SIPI. Penulis telah menyusun beberapa saran yang dapat dijadikan sebagai langkah yang dapat diambil untuk meningkatkan tingkat keamanan *website* terhadap jenis serangan *packet sniffing* pada kedua *platform* ini.

1. Pengguna *Website*

- a) Menerapkan keamanan enkripsi WPA2-PSK pada *hotspot* untuk meningkatkan keamanan. Dengan menerapkan keamanan tersebut, hanya pengguna yang memiliki akses yang dapat mengakses jaringan. Sehingga, serangan *sniffing* oleh pihak yang tidak berwenang dapat cegah.
- b) Menghindari pengaksesan akun atau mengirim data sensitif saat menggunakan jaringan *hotspot* umum atau *hotspot* yang kata sandinya banyak yang tahu. Hal ini dapat menjadi peluang lebih besar untuk menjadi target serangan *sniffing*.

2. Pengembang Situs Web

- a) Melakukan penerapan sertifikat SSL pada *website* Sigmatik dan SIPI. Dengan mengaktifkan sertifikat SSL, informasi yang bersifat rahasia akan tetap terlindungi saat dikirim melalui internet karena akan diubah menjadi format terenkripsi. Akibatnya, hanya penerima pesan yang memiliki kunci dekripsi yang dapat membaca isi pesan tersebut setelah melewati proses enkripsi. Tindakan ini menjadi sangat penting karena pada saat data dikirimkan melalui perjalanan ke beberapa komputer sebelum mencapai server tujuan. Jika tidak ada enkripsi dengan sertifikat SSL, perangkat lain yang berada di antara komputer pengguna dan server dapat mengakses data sensitif seperti nama pengguna dan kata sandi.

BAB V

PENUTUP

A. Kesimpulan

Dari temuan yang diungkapkan dalam penelitian ini, dapat diambil kesimpulan sebagai berikut:

1. Tingkat keamanan *website* di Jurusan Teknik Informatika dan Komputer masih memerlukan peningkatan pada *website* Sigmatik, dan SIPI. Hal ini terbukti karena *website* tersebut rentan terhadap serangan *packet sniffing* yang memiliki kemampuan untuk merekam dan menampilkan informasi sensitif seperti *Username* dan *password* saat proses *login* dilakukan menggunakan aplikasi *Wireshark*. Pada *website* Sigmatik, dan SIPI belum menerapkan sertifikat SSL seperti *website* SIMPEL, SIM-TA, dan IDS. Oleh karena itu, sangat rentan terhadap serangan *packet sniffing*, meskipun jika *User* menggunakan versi terbaru dari *browser*.
2. Hasil identifikasi dari serangan *packet sniffing* pada *website* di Jurusan Teknik Informatika dan Komputer yaitu mendapatkan informasi berupa jenis koneksi dan protokol yang digunakan, jenis pesan seperti POST dan GET, jenis *port*, *host* atau server, jenis *browser* yang digunakan, Bahasa, jenis server yang digunakan, serta yang paling penting informasi data sensitif seperti *Username* dan *password User*.

B. Saran

Berdasarkan uraian dari kesimpulan, maka kelemahan yang telah diidentifikasi dapat dijadikan sebagai pengalaman dan referensi untuk kedepannya. Untuk itu, rekomendasi dari penulis untuk penelitian selanjutnya yaitu dapat merancang sistem pemantauan dan deteksi yang dapat dengan cepat mengenali potensi serangan *packet sniffing*, sehingga langkah-langkah untuk menangani masalah tersebut dapat segera ditindak lanjuti, seperti implementasi *Intrusion Prevention System* (IPS) yang dirancang untuk mendeteksi serangan, serta dapat mengambil tindakan pencegahan untuk memblokir serangan tersebut secara otomatis.

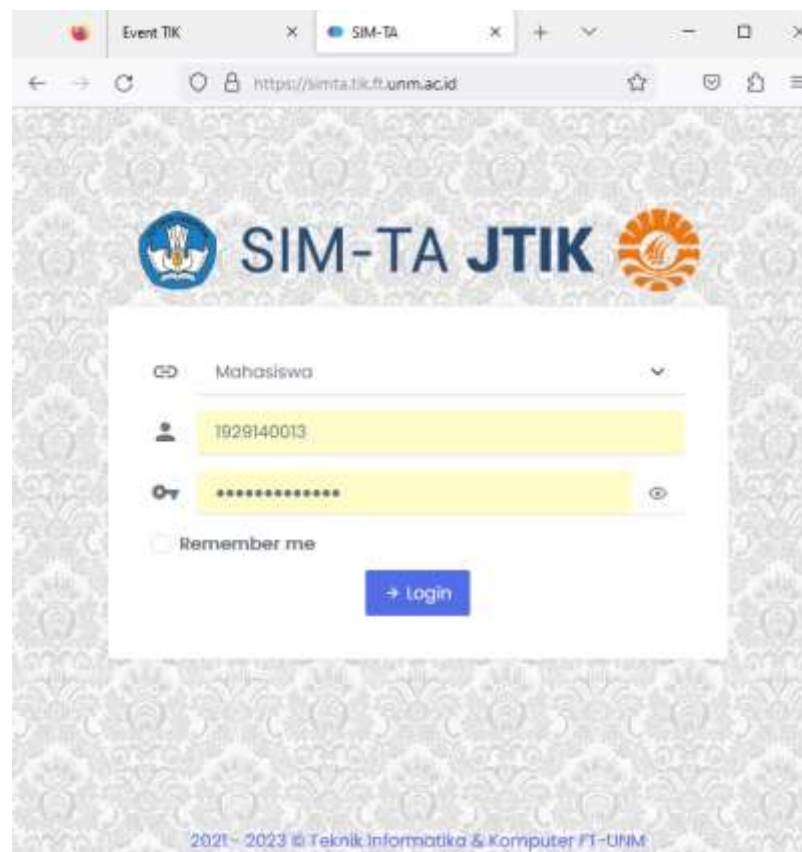
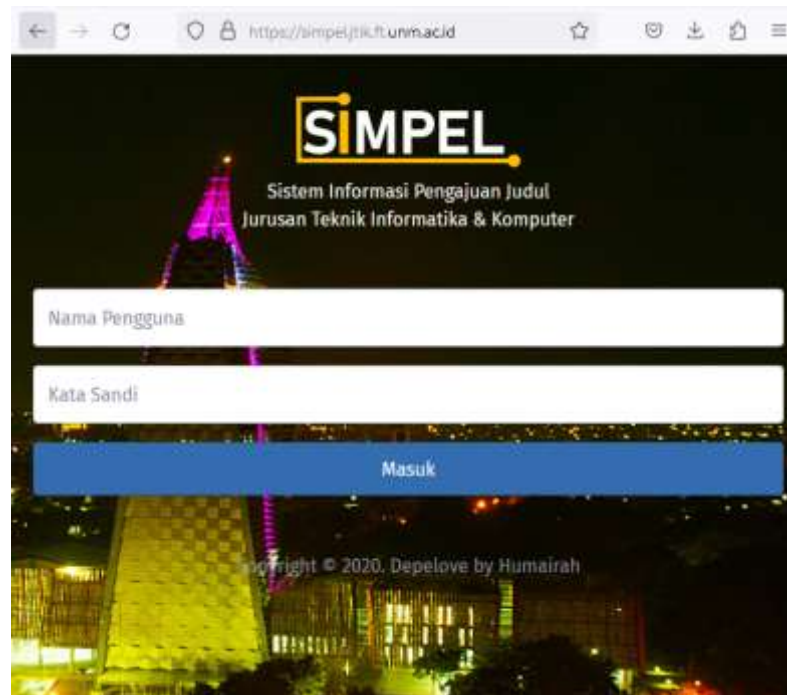
DAFTAR PUSTAKA

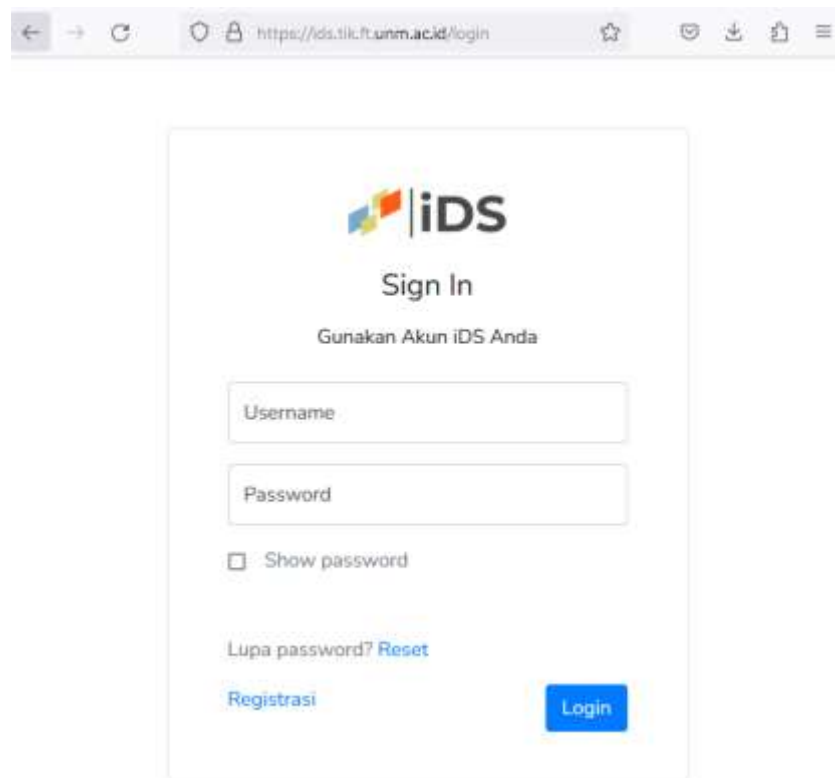
- Abdillah, M. A., Yudhana, A., & Fadil, A. (2020). *Sniffing Pada Jaringan Wi-Fi Berbasis Protokol 802.1x Menggunakan Aplikasi Wireshark. J-SAKTI (Jurnal Sains Komputer dan Informatika)*, 4(1), 1.
- Arini, N. E. (2010). *Bahan Ajar : Materi Psikologi Eksperimen*.
- Futra, Y. (2020). Tinjauan Peristiwa *Cyber Crime* Yang Terjadi Pada Tahun 2019 Di Kota Sawahlunto. *UNES Law Review*, 3(1), 55–68.
- Gondohanindijo, J. (2012). Sistem Keamanan Jaringan Nirkabel. *Majalah Ilmiah Informatika*, 3(2), 141–160.
- Hidayat, M. T., Sn, F. M., & Kurniati, N. I. (2018). Analisis Keamanan Jaringan Pada Fasilitas Internet (Wi-Fi) Gratis Terhadap Serangan *Packet sniffing*. *Scientific Articles of Informatics Students*, 1(2), 112–119.
- Jamaluddin, H., & Suaeb, N. F. (2018). Analisis Keamanan Website Terhadap Sniffing Process Pada Jaringan Nirkabel Menggunakan Aplikasi Wireshark (Studi Kasus: Simak Unismuh).
- Kristiyanti, M. (2010). Internet Sebagai Media Pembelajaran Yang Efektif. *Majalah Ilmiah Informatika*, 1(1), 8–29.
- Kurniawan, T. A. (2020). Analisa Keamanan Jaringan Wi-Fi Terhadap Serangan *Packet Sniffing*. *Jurnal Ilmiah Fakultas Teknik LIMIT'S*, 16(2), 11–15.
- Lamada, M. S., Miru, A. S., & Amalia, R.-. (2020). Pengujian Aplikasi Sistem Monitoring Perkuliahan Menggunakan Standar ISO 25010. *Jurnal MediaTIK*, 3(3). <https://doi.org/10.26858/jmtik.v3i3.15172>
- Mutaqin, A. F. (2016). Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort. *Jurnal Sistem dan Teknologi Informasi (JUSTIN)*, 1(1), 1–6.
- Qadeer, M. A., Iqbal, A., Zahid, M., & Siddiqui, M. R. (2010). *Network Traffic Analysis and Intrusion Detection Using Packet Sniffer*. 2010 *Second International Conference on Communication Software and Networks*, 313–317. <https://doi.org/10.1109/ICCSN.2010.104>
- Rochmawati, I. (2019). *Iwearup.Com User Interface Analysis*. *Visualita*, 7(2), 31–44. <https://doi.org/10.33375/vslt.v7i2.1459>

- Rodhin, R. (2012). Internet Dalam Konteks Perpustakaan. *Pustakaloka*, 4(1), 1–19.
- Siahaan, A. P. U. (2018). Pelanggaran *Cybercrime* Dan Kekuatan Yurisdiksi Di Indonesia. *Jurnal Teknik Dan Informatika*, 5(1), 6–9.
- Sutanto, Y. (2015). Analisis Kepuasan Pengguna *Website* Manajemen Informatika Dengan Metode Eucs Berbasis Cms. *Informatika*, 2(1), 1–18.
- Syahaab, A. S., Ujianto, E. I. H., & Rianto, R. (2023). Penggunaan *Wireshark* Dan *Nessus* Untuk Analisis Ssl/Tls Pada Keamanan Data Pengguna *Website*. *Jika (Jurnal Informatika)*, 7(2), 183. <https://doi.org/10.31000/jika.v7i2.7566>
- Syaifuddin, M., Andika, B., & Ginting, R. I. (2017). Analisis Celah Keamanan Protocol TCP/IP. *Jurnal Ilmiah SAINTIKOM*, 16(2), 130–135.
- Wati, E. S., & Apriansyah, D. (2019). Sistem Keamanan Jaringan *Wireless* Menggunakan Peap Ms Chap. *Jurnal ONESISMIK*, 1(1), 1–9.




LAMPIRAN

Lampiran 1. 1 Hasil Uji Coba Serangan *Packet Sniffing***TAMPILAN WEBSITE JTIK**



← → ↻ 🔒 https://ids.tik.ft.unm.ac.id/login ☆ 🛡️ 📄 ☰



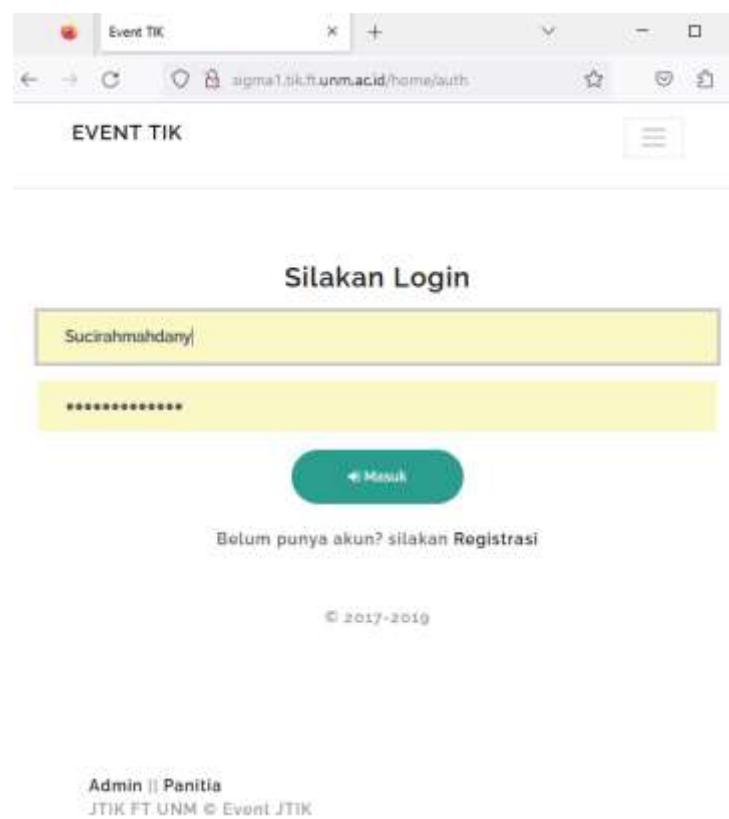
Sign In

Gunakan Akun iDS Anda

☐ Show password

Lupa password? [Reset](#)

[Registrasi](#) [Login](#)



Event TIK × + - □

← → ↻ 🔒 sigma1.tik.ft.unm.ac.id/home/auth ☆ 🛡️ 📄 ☰

EVENT TIK ☰

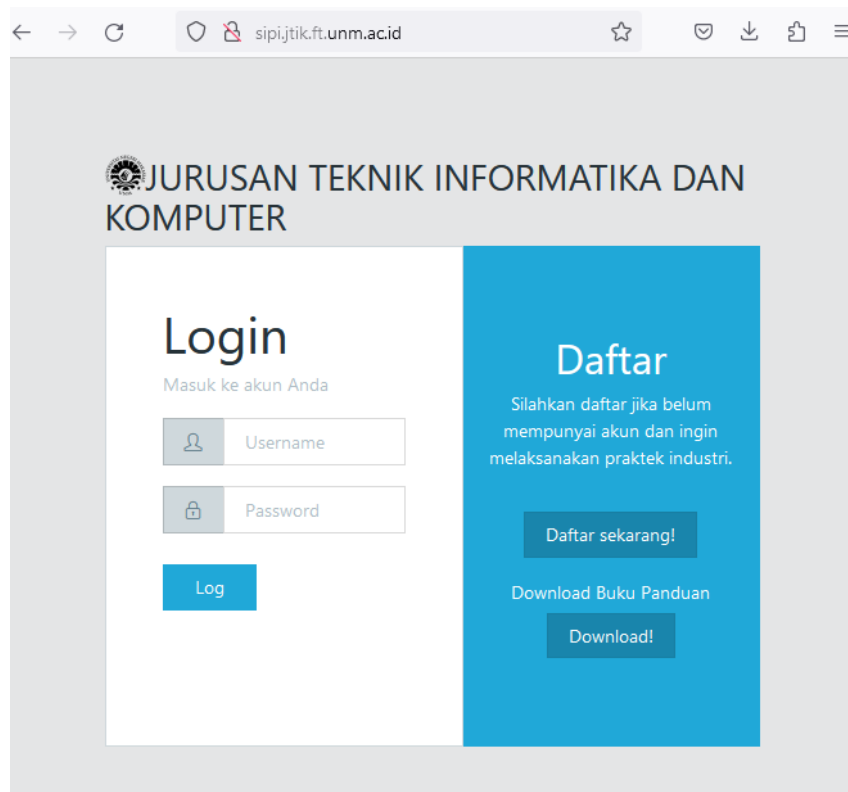
Silakan Login

[← Masuk](#)

Belum punya akun? silakan [Registrasi](#)

© 2017-2019

Admin || Panitia
JTIK FT UNM © Event JTIK



The screenshot shows a web browser window with the address bar displaying `sipi.jtik.ft.unm.ac.id`. The page header features the logo of Universitas Negeri Makassar and the text "JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER". The main content area is divided into two sections: "Login" and "Daftar".

Login
Masuk ke akun Anda

Username

Password

Log

Daftar
Silahkan daftar jika belum mempunyai akun dan ingin melaksanakan praktek industri.

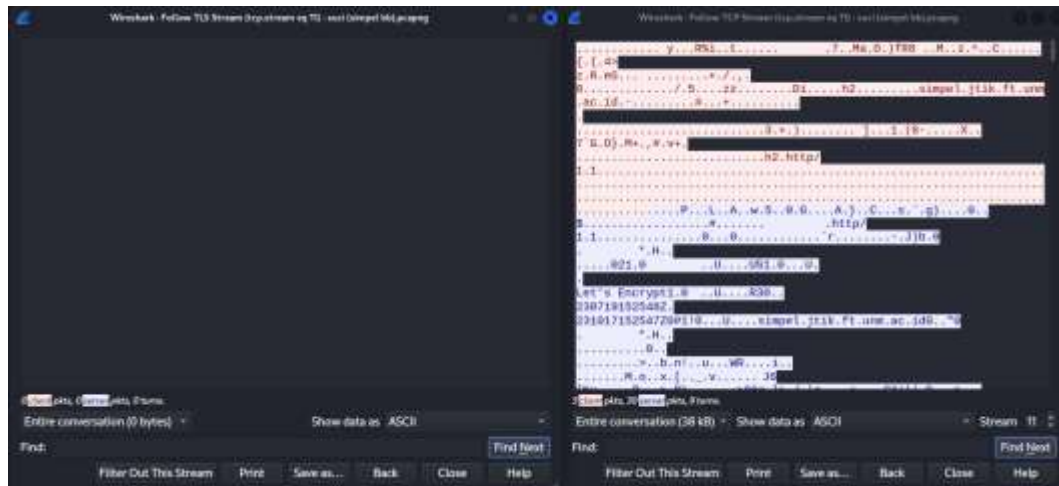
Daftar sekarang!

Download Buku Panduan

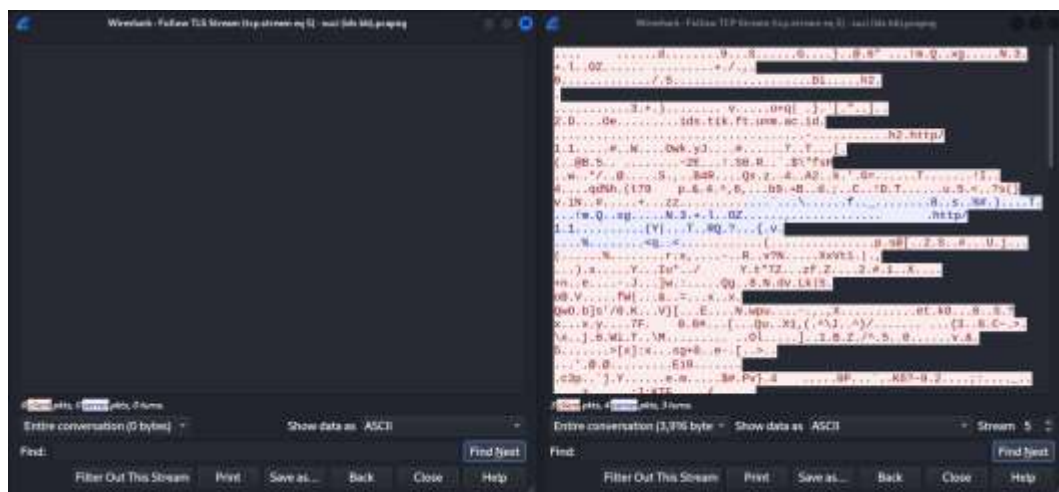
Download!

1. *User 1* (192.168.1.47)

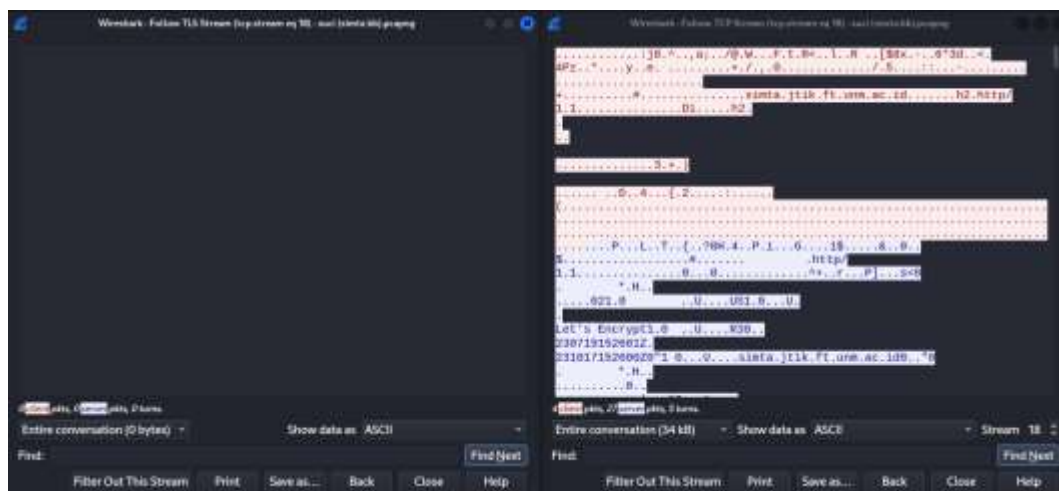
SIMPEL



IDS



SIMTA



Sigmatik

```

Wireshark - Follow HTTP Stream (tcp.stream eq 6) - sigma1.pcapng

Host: sigma1.tik.ft.unm.ac.id
Connection: keep-alive
Content-Length: 46
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://sigma1.tik.ft.unm.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/116.0.0.0 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://sigma1.tik.ft.unm.ac.id/home/auth
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: __dtsu=4C3016907895933965CCC4C5B048B153;
_cc_id=1c9438bb5ac71126880ec069e5417ae2; panoramaId_expiry=1693285360094;
panoramaId=3b71c597df3334ab3eba3464887ba9fb927a705944263a4261dae641bff01983;
panoramaIdType=panoDevice; ci_session=0cf2074a7f0109657712582e402c5f0a0c420626

username=Sigma1&password=Sigma1 HTTP/1.1 200 OK
Date: Mon, 28 Aug 2023 05:49:58 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Refresh: 0;url=http://sigma1.tik.ft.unm.ac.id/home
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

GET /home HTTP/1.1

```

SIPI

```

Wireshark - Follow HTTP Stream (tcp.stream eq 62) - eth0

POST /login/do_login HTTP/1.1
Host: sipi.jtik.ft.unm.ac.id
Connection: keep-alive
Content-Length: 44
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://sipi.jtik.ft.unm.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/116.0.0.0 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://sipi.jtik.ft.unm.ac.id/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=75995f24e413774dbffd2dfac6bba58d18376d35

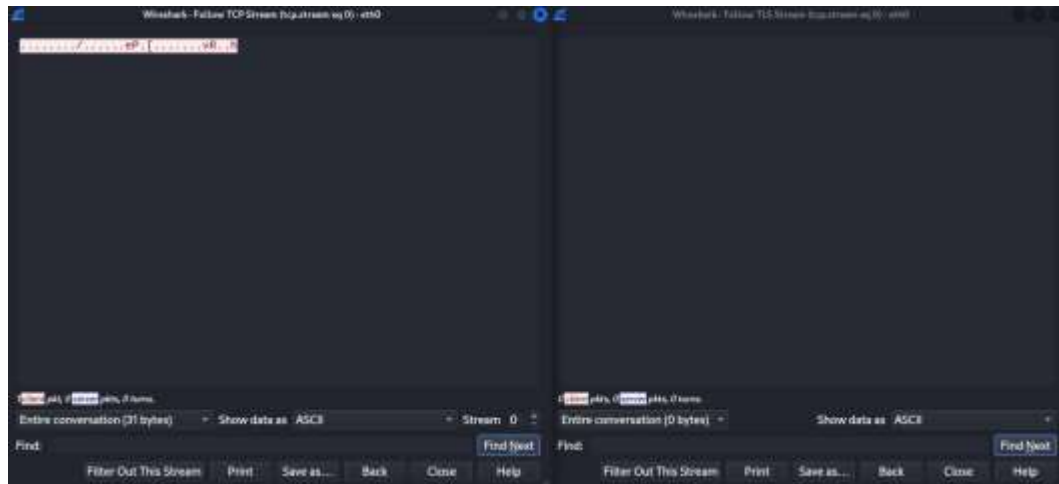
username=Sigma1&password=Sigma1 HTTP/1.1 200 OK
Date: Sun, 10 Sep 2023 07:08:12 GMT
Server: Apache/2.4.48 (Unix) OpenSSL/1.0.2k-fips
X-Powered-By: PHP/5.6.37
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Refresh: 0;url=http://sipi.jtik.ft.unm.ac.id/dashboard

3 client pkts, 3 server pkts, 5 turns.
Entire conversation (15 kB)
Show data as ASCII
Find:
Filter Out This Stream Print Save as... Back Close Help

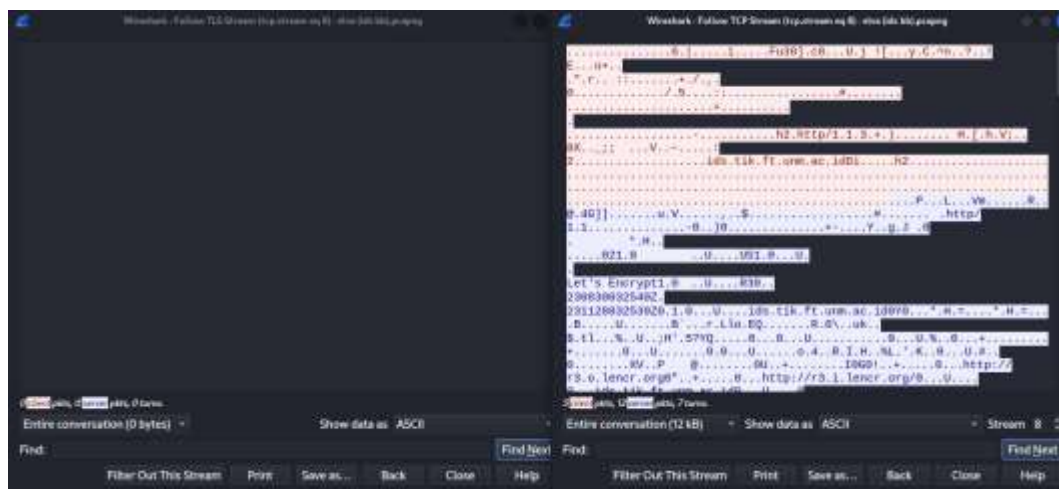
```


2. User 2 (192.168.1.74)

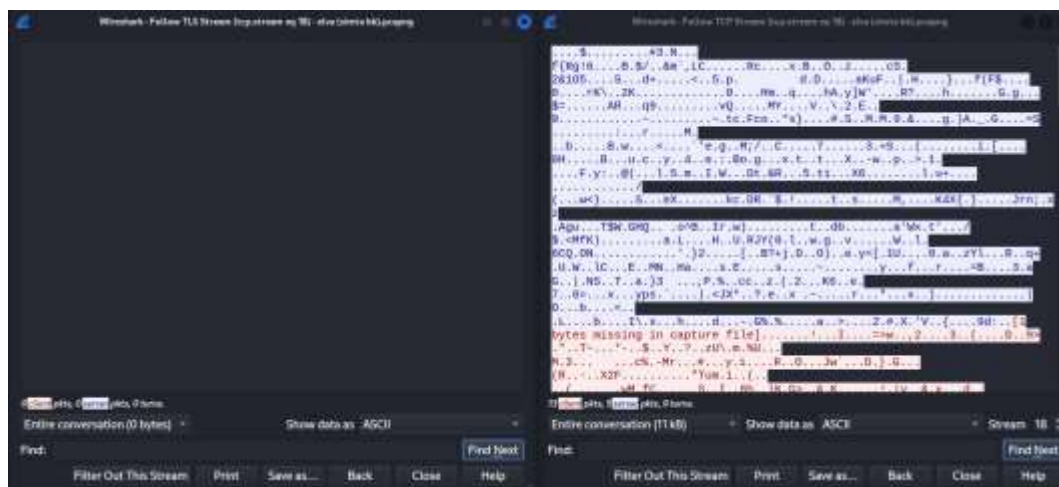
SIMPEL



IDS



SIMTA



Sigmatik

```

Origin: http://sigma1.tik.ft.unm.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/116.0.0.0 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://sigma1.tik.ft.unm.ac.id/home/auth
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: _ga_4HT7TCYTDP=GS1.1.1673597975.26.0.1673597975.0.0.0;
_ga_J1DQF09WZC=GS1.3.1691402067.3.0.1691402067.0.0.0;
_ga=GA1.1.1151097940.1613971455;
_ga_5P0T6NWDWX=GS1.1.1693319224.639.1.1693319225.0.0.0;
ci_session=8b4d9a52b89e68787a0a5db788beb3c975756a3a

username=&password=& HTTP/1.1 200 OK
Date: Wed, 06 Sep 2023 07:04:42 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Refresh: 0;url=http://sigma1.tik.ft.unm.ac.id/home
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

```

2 client pkts, 2 server pkts, 3 turns.

Entire conversation (8,659 bytes) Show data as ASCII

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

SIPI

```

POST /login/do_login HTTP/1.1
Host: sipi.jtik.ft.unm.ac.id
Connection: keep-alive
Content-Length: 32
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://sipi.jtik.ft.unm.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/116.0.0.0 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://sipi.jtik.ft.unm.ac.id/login
Accept-Encoding: gzip, deflate
Accept-Language: id,id-ID;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: _ga=GA1.3.765949052.1691537030; perf_dv6Tr4n=1;
PHPSESSID=929b82568f1d4b662dd07712a755727906714096;
_gid=GA1.3.1791999407.1694504493;
_ga_J1DQF09WZC=GS1.3.1694504494.6.1.1694504521.0.0.0

username=1&password=2 HTTP/1.1 200 OK
Date: Mon, 11 Sep 2023 08:06:18 GMT
Server: Apache/2.4.48 (Unix) OpenSSL/1.0.2k-fips
X-Powered-By: PHP/5.6.37
Expires: Thu, 19 Nov 1981 08:52:00 GMT

```

3 client pkts, 3 server pkts, 5 turns.

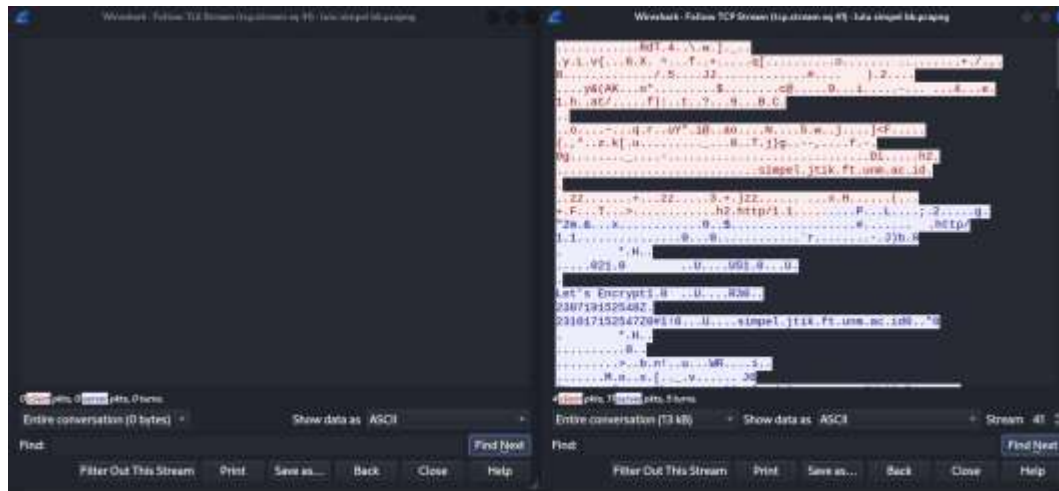
Entire conversation (16 kB) Show data as ASCII

Find: Find Next

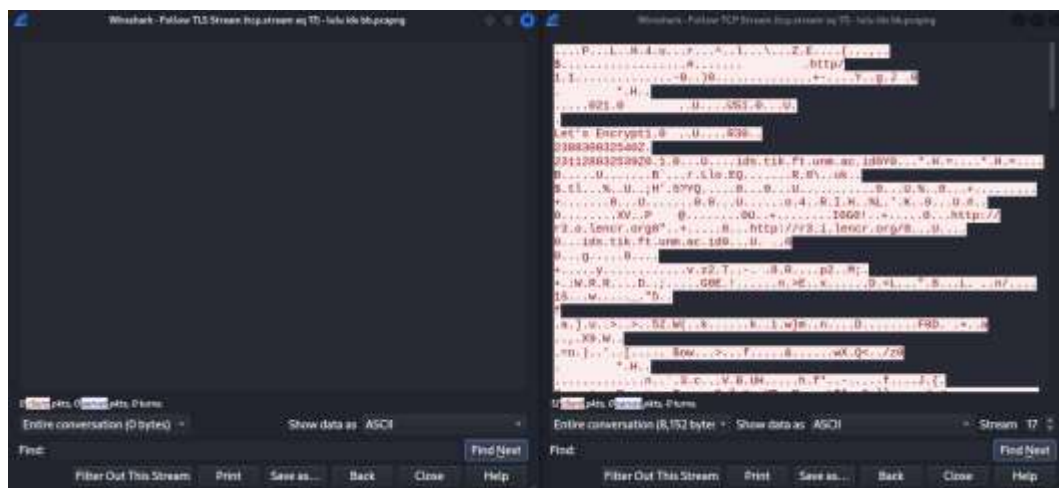
Filter Out This Stream Print Save as... Back Close Help

3. User 3 (192.168.1.27)

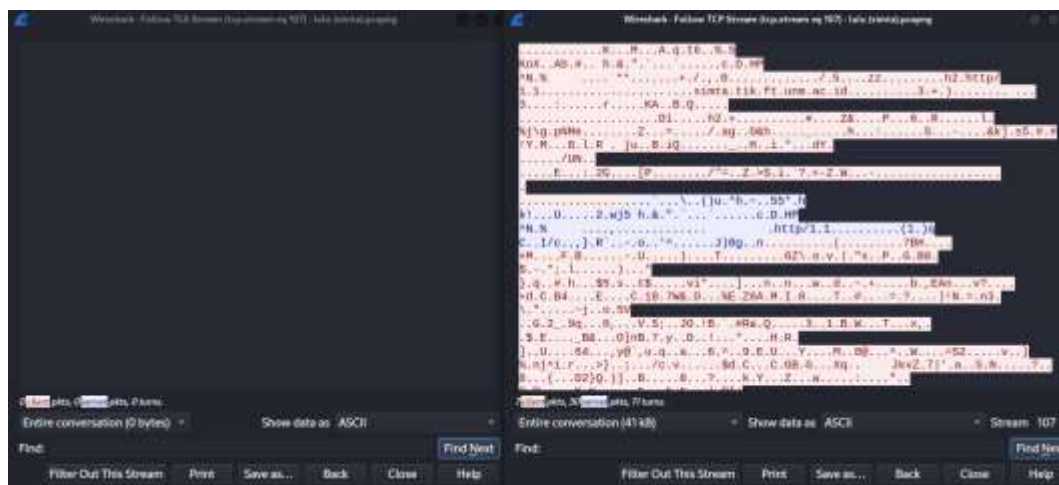
SIMPEL



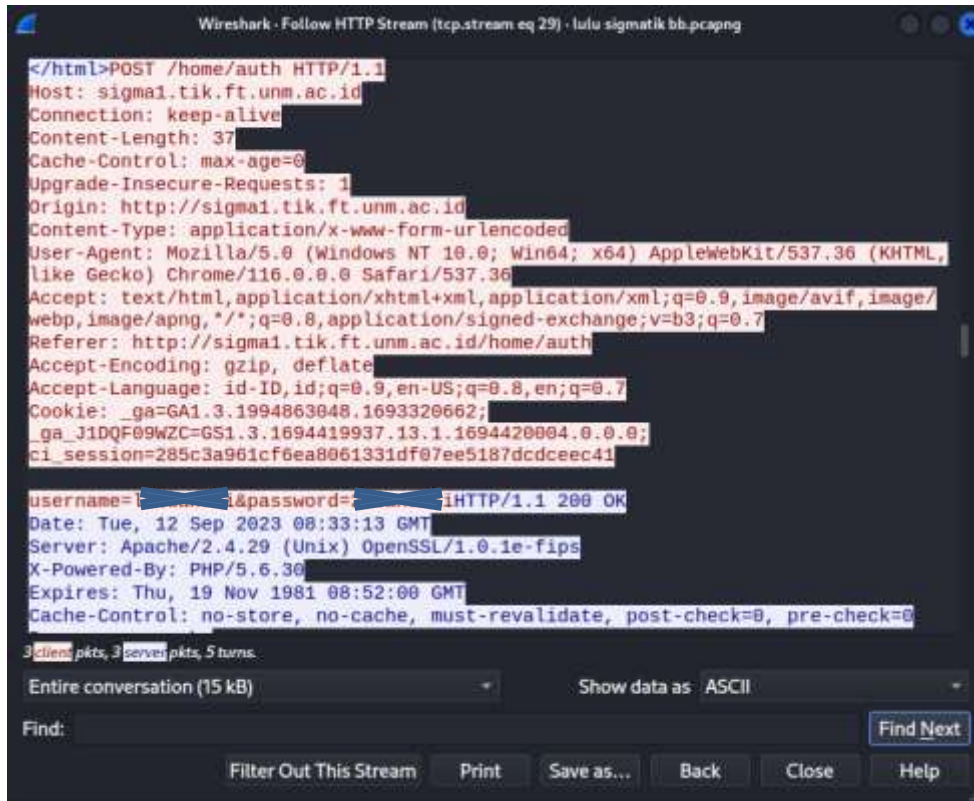
IDS



SIMTA



Sigmatik



```

Wireshark - Follow HTTP Stream (tcp.stream eq 29) - lulu sigmatik bb.pcapng

</html>POST /home/auth HTTP/1.1
Host: sigma1.tik.ft.unm.ac.id
Connection: keep-alive
Content-Length: 37
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://sigma1.tik.ft.unm.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/116.0.0.0 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://sigma1.tik.ft.unm.ac.id/home/auth
Accept-Encoding: gzip, deflate
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: _ga=GA1.3.1994863048.1693320662;
_ga_J1DQF09WZC=GS1.3.1694419937.13.1.1694420004.0.0.0;
ci_session=285c3a961cf6ea8061331df07ee5187dcdceec41

username=&password=&iHTTP/1.1 200 OK
Date: Tue, 12 Sep 2023 08:33:13 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

3 client pkts, 3 server pkts, 5 turns.
Entire conversation (15 kB)
Show data as ASCII
Find: Find Next
Filter Out This Stream Print Save as... Back Close Help

```

SIPI



```

Wireshark - Follow HTTP Stream (tcp.stream eq 19) - eth0

POST /login/do_login HTTP/1.1
Host: sipi.jtik.ft.unm.ac.id
Connection: keep-alive
Content-Length: 38
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://sipi.jtik.ft.unm.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/116.0.0.0 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://sipi.jtik.ft.unm.ac.id/login
Accept-Encoding: gzip, deflate
Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: _ga=GA1.3.1994863048.1693320662;
_ga_J1DQF09WZC=GS1.3.1694419937.13.1.1694420004.0.0.0;
PHPSESSID=876cbe1c0ffe61fedb70d18824478903fa9c1ab7

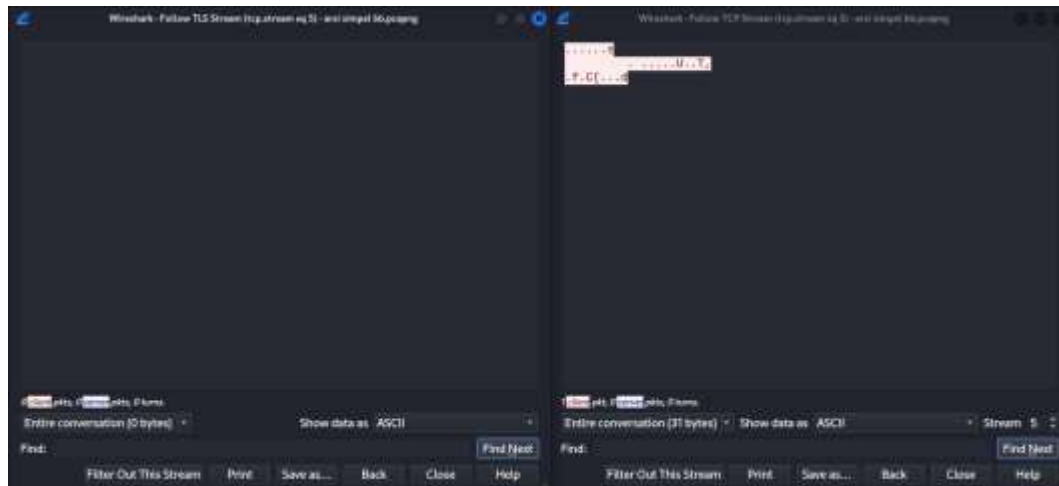
username=&/&password=&iHTTP/1.1 200 OK
Date: Tue, 12 Sep 2023 08:37:20 GMT
Server: Apache/2.4.48 (Unix) OpenSSL/1.0.2k-fips
X-Powered-By: PHP/5.6.37
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

2 client pkts, 1 server pkt, 2 turns.
Entire conversation (1,998 bytes)
Show data as ASCII
Find: Find Next
Filter Out This Stream Print Save as... Back Close Help

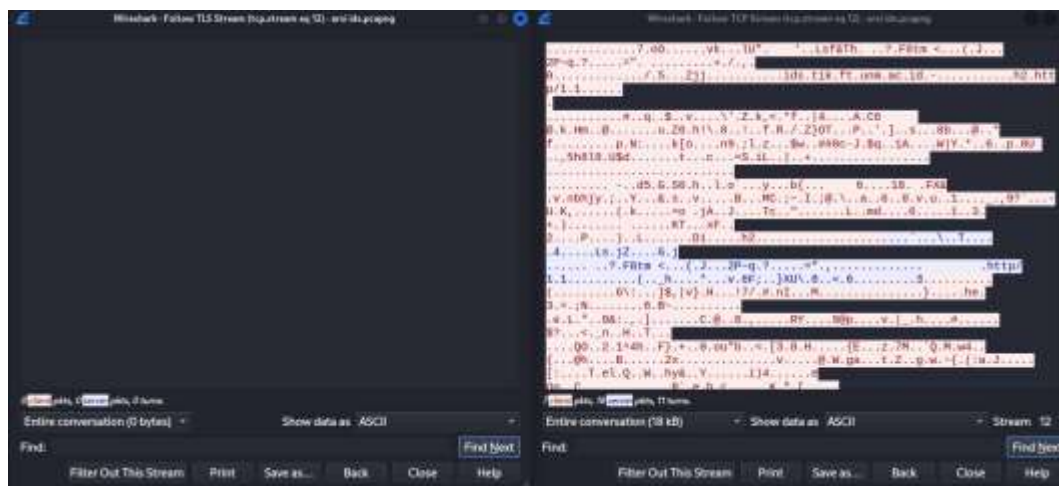
```


4. *User 4 (192.168.1.63)*

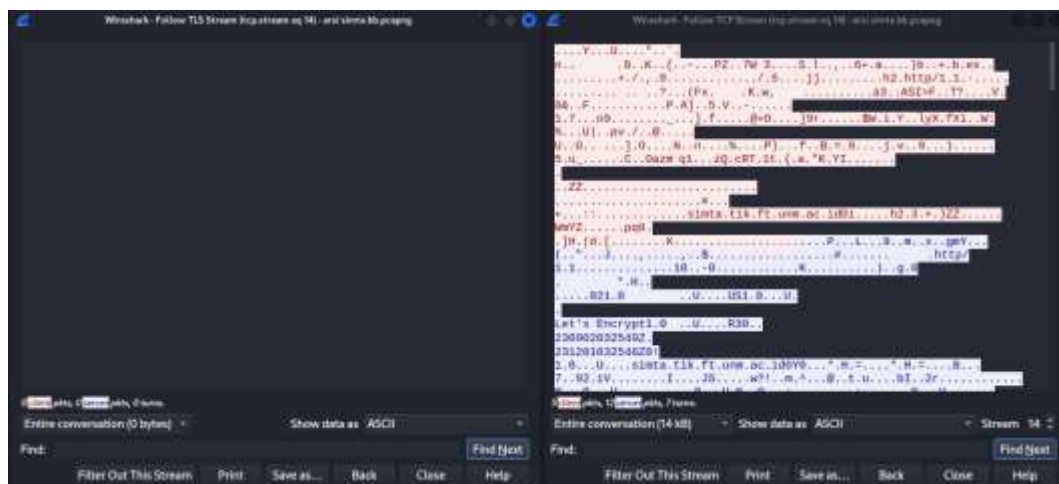
SIMPEL



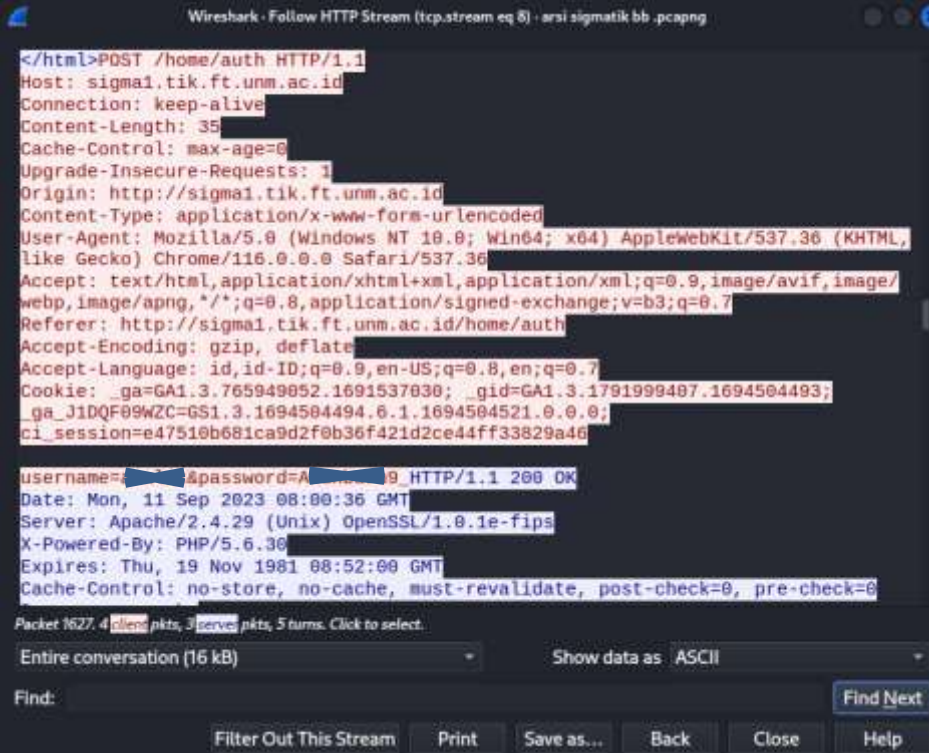
IDS



SIMTA



Sigmatik



```

Wireshark · Follow HTTP Stream (tcp.stream eq 8) · arsi sigmatik bb.pcapng

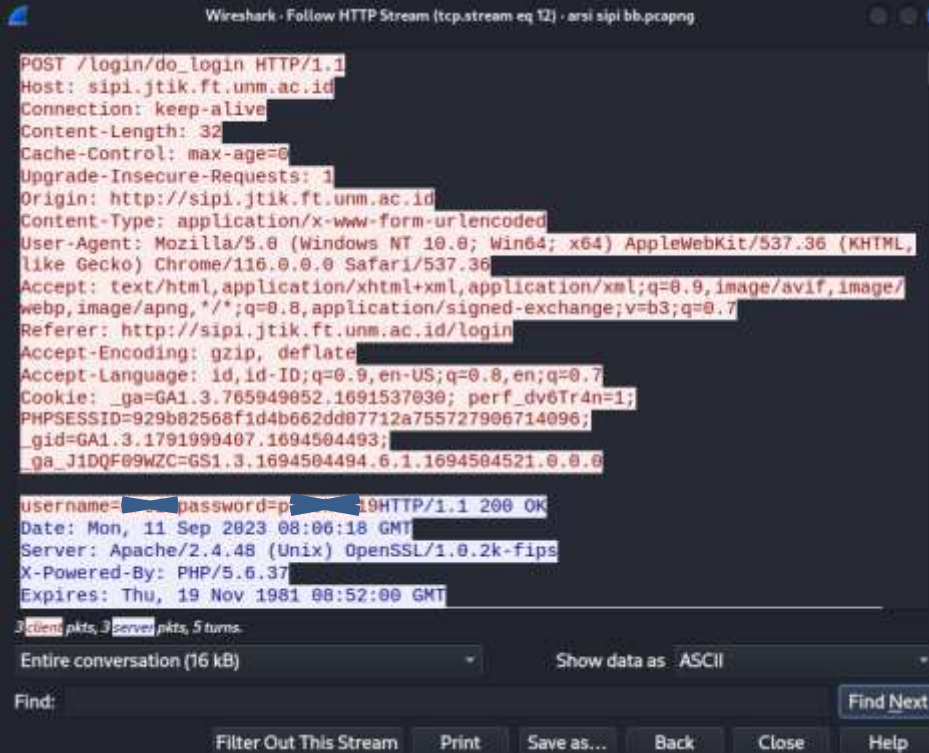
</html>POST /home/auth HTTP/1.1
Host: sigma1.tik.ft.unm.ac.id
Connection: keep-alive
Content-Length: 35
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://sigma1.tik.ft.unm.ac.id
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/116.0.0.0 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://sigma1.tik.ft.unm.ac.id/home/auth
Accept-Encoding: gzip, deflate
Accept-Language: id,id-ID;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: _ga=GA1.3.765949052.1691537030; _gid=GA1.3.1791999407.1694504493;
_ga_J1DQF09WZC=GS1.3.1694504494.6.1.1694504521.0.0.0;
ci_session=e47510b681ca9d2f0b36f421d2ce44ff33829a46

username=&password=A HTTP/1.1 200 OK
Date: Mon, 11 Sep 2023 08:00:36 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.1e-fips
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Packet 1627: 4 client pkts, 3 server pkts, 5 turns. Click to select.
Entire conversation (16 kB) Show data as ASCII
Find: Find Next
Filter Out This Stream Print Save as... Back Close Help

```

SIPI



```

Wireshark · Follow HTTP Stream (tcp.stream eq 12) · arsi sipi bb.pcapng

POST /login/do_login HTTP/1.1
Host: sipi.jtik.ft.unm.ac.id
Connection: keep-alive
Content-Length: 32
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://sipi.jtik.ft.unm.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/116.0.0.0 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://sipi.jtik.ft.unm.ac.id/login
Accept-Encoding: gzip, deflate
Accept-Language: id,id-ID;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: _ga=GA1.3.765949052.1691537030; perf_dv6Tr4n=1;
PHPSESSID=929b02568f1d4b662dd07712a755727906714096;
_gid=GA1.3.1791999407.1694504493;
_ga_J1DQF09WZC=GS1.3.1694504494.6.1.1694504521.0.0.0

username=&password=p HTTP/1.1 200 OK
Date: Mon, 11 Sep 2023 08:06:18 GMT
Server: Apache/2.4.48 (Unix) OpenSSL/1.0.2k-fips
X-Powered-By: PHP/5.6.37
Expires: Thu, 19 Nov 1981 08:52:00 GMT

3 client pkts, 3 server pkts, 5 turns.
Entire conversation (16 kB) Show data as ASCII
Find: Find Next
Filter Out This Stream Print Save as... Back Close Help

```

Lampiran 1. 2 PersuratanLampiran 1. 3 Persuratan



KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
Alamat: JL. Daeng Tata Raya Parangtambung Makassar – 90224
Telp. 0411-864935, Fax. 0411 – 861507, HP. 0853-1122-4040
Email: jtik@unm.ac.id | Laman jtik.ft.unm.ac.id

PERMOHONAN JUDUL SKRIPSI

A. Identitas Mahasiswa

1. Nama : Suci Rahmadany
2. NIM : 1929140013
3. Program Studi : Teknik Komputer - (S1)
4. Jurusan : Teknik Informatika dan Komputer

B. Judul yang diajukan:

1. Analisis Keamanan Jaringan pada Fasilitas Internet (*Wifi* SSO-UNM) Terhadap Serangan Packet Sniffing di Fakultas Teknik Universitas Negeri Makassar.
2. Analisis Sistem Keamanan Jaringan *Wifi* SSO-UNM menggunakan *Wireshark* pada Fakultas Teknik Universitas Negeri Makassar.
3. Implementasi Proxy dan Snort Sebagai *Gateway* Antivirus.

Dosen Penasehat Akademik,

Dr. Mustari Lamada, S.Pd., M.T.
NIP. 19750505-200501-1-001

Mahasiswa,

Suci Rahmadany
NIM. 1929140013

Mengetahui,
Ketua Prodi Teknik Komputer

Dr. Satria Gunawan Zain, S.Pd., M.T.
NIP. 19800809-201012-1-002



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR (UNM)
FAKULTAS TEKNIK

Alamat: Jalan Daeng Tata Raya Parangtambung Makassar

Telp (0411) 865677 Fax. (0411) 861377

Laman: fl.unm.ac.id

Nomor : 2516/UN36.2/PP/2023

10 Agustus 2023

Hal : Penunjukan Sebagai Pembimbing/
Konsultasi Skripsi/TA

Yth : 1.Dr. Ir. Mustari S. Lamada, S.Pd., M.T.

(Pembimbing I)

: 2.Dr. Hendra Jaya, S.Pd., M.T.

(Pembimbing II)

Dosen Fakultas Teknik Universitas Negeri Makassar

Dalam rangka penulisan Skripsi mahasiswa di bawah ini:

Nama : Suci Rahmadany

NIM : 1929140013

Jurusan : Teknik Informatika dan Komputer

Program Studi : Teknik Komputer - S1

Diminta kesediaan Saudara untuk menjadi pembimbing/konsultan dalam penulisan Skripsi dengan judul sementara:

"Analisis Keamanan Website terhadap Serangan Packet Sniffing di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar"

Judul tersebut masih dapat didiskusikan antara Saudara dengan Mahasiswa yang bersangkutan. Maksimal waktu pembimbingan 6 (enam) bulan terhitung dari tanggal dikeluarkannya SK pembimbingan hingga siap ujian akhir. Jika dalam waktu tersebut proses pembimbingan belum selesai, maka tugas yang diberikan kepada Saudara akan ditinjau kembali.

Kiranya sebelum penulisan Skripsi Mahasiswa tersebut lebih dahulu memasukkan Kerangka Skripsi yang ditulis dan Saudara setuju untuk kami ketahui.

Atas kesediaan dan perhatian diucapkan terima kasih.

a.n Dekan

Wakil Dekan Bidang Akademik



Prof. Dr. Drs. Ir. Jamaluddin P, MP., IPM.

NIP. 196707231992031002

*dokumen ini ditandatangani secara elektronik yang dapat diverifikasi melalui laman resmi my-sigma.fl.unm.ac.id



KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

Alamat: Jl. Daeng Tata Raya Parangtambung Makassar – 90224

Telp. 0411-864935, Fax. 0411 – 861507, HP. 0853-1122-4040, Email: jtik@unm.ac.id | Laman tik.fl.unm.ac.id

NAMA / NIM : Suci Rahmahdany / 1929190013

JUDUL SKRIPSI : Analisis Keamanan Jaringan pada Fasilitas Internet (Wi-Fi SSO-UNM)
Terhadap Serangan Paket Sniffing di Fakultas Teknik UNM.

PEMBIMBING : Dr. MUSTARI S. LAMADA, M.T.

No.	TANGGAL	DESKRIPSI MATERI PEMBIMBINGAN	PARAF PEMBIMBING
1.	14/01/2023	- Mengevaluasi usulan proposal - Cek typo, tanda baca dan lain-lain	
2.	17/01/2023	- Cek kerapian usulan - Usulan beberapa kata kunci	
2.	24/01/2023	- Perjelas aplikasi yang apa saja dan di mana	
3.	24/01/2023	- Pelajari aplikasi yang apa saja dan di mana	
3.	9/02/2023	- Rapihkan usulan - Sebutkan di prosedur penelitian yang sudah - Rapihkan tulisan, cek typo - Tambah teori pendahuluan di bagian pendahuluan - Daftar pustaka	

Dr. Mustari Lamada, S.Pd., M.T.
NIP. 19750505 200501 1 001

CATATAN:

1. Kartu bimbingan dibawa setiap kali konsultasi dengan pembimbing
2. Kartu bimbingan dicetak pada kertas karton; untuk proposal (warna orange), untuk hasil (warna hijau muda)



KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
UNIVERSITAS NEGERI MAKASSAR

FAKULTAS TEKNIK

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

Alamat: Jl. Daeng Tata Raya Parangtambung Makassar - 90224

Telp. 0411-864935, Fax. 0411-861507, HP. 0853-1122-4040, Email. jtik@unm.ac.id | Laman tik.fl.unm.ac.id

NAMA / NIM : Suci Rahmawati / 1929190023

JUDUL SKRIPSI :

PEMBIMBING : Dr. MUSTARI S. LAMADA, M.T.

No	TANGGAL	DESKRIPSI MATERI PEMBIMBINGAN	PARAF PEMBIMBING
4.	19/02/2023	- Silahkan Ubah judulnya - cek typo - Rumusan masalah adalah - Pertanyaan penelitian yang akan - Diteliti jawabannya - cek Paragraf jawab	
5.	28/02/2023	- Daftar Isi - cek typo - Rumusan Masalah - Perbaiki masalah	
6.	2/03/2023	- cek margin awal - Mayu Seapero - Buat PPT	

Pembimbing

Dr. Mustari Lamada, S.Pd., M.T.
NIP. 19750505 200501 1 001

CATATAN:

1. Kartu bimbingan dibawa setiap kali konsultasi dengan pembimbing
2. Kartu bimbingan dicetak pada kertas karton; untuk proposal (warna orange), untuk hasil (warna hijau muda)



**KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK**

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

Alamat: Jl. Daeng Tata Raya Parangtambung Makassar – 90224

Telp. 0411-864935, Fax. 0411 – 861507, HP. 0853-1122-4040, Email: jtik@unm.ac.id | Laman tik.fl.unm.ac.id

LEMBAR KONSULTASI SKRIPSI

Nama : SUCI RAHMAHDANY
NIM : 1929140013
Prodi : TEKNIK KOMPUTER
Judul : Analisis Keamanan Jaringan pada Fasilitas Internet (WiFi SSO-UNM)
Terhadap Serangan Packet Sniffing di Fakultas Teknik Universitas Negeri Makassar

Pembimbing I : Dr. Mustari S. Lamada, S.Pd. M.T.
Pembimbing II : Dr. Hendra Jaya, M.T

No	Tanggal	Keterangan	Paraf
1.	1/12-2021	Bab I	
2.	2/12-2021	Bab II, Dst pda	
3	14/02-22	Bab III, - Dst pda. - Prosed politiz	
4	28/02-23	Tela paku.	

Pembimbing II

Dr. Hendra Jaya, M.T
NIP. 198209072005011001



KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

Alamat: JL. Daeng Tata Raya Parangtambung Makassar – 90224

Telp. 0411-864935, Fax. 0411 – 861507, HP 0853-1122-4040, Email jtik@unm.ac.id | Laman.tik.ft.unm.ac.id

LEMBAR KONSULTASI SKRIPSI

Nama : SUCI RAHMAHDANY
NIM : 1929140013
Prodi : TEKNIK KOMPUTER
Judul : Analisis Keamanan Jaringan pada Fasilitas Internet (WiFi SSO-UNM)
Terhadap Serangan Packet Sniffing di Fakultas Teknik Universitas Negeri
Makassar

Pembimbing I : Dr. Mustari S. Lamada, S.Pd. M.T.
Pembimbing II : Dr. Hendra Jaya, M.T

No	Tanggal	Keterangan	Paraf
1	3/mar 2023	PUU Propon	

Pembimbing II

Dr. Hendra Jaya, M.T
NIP. 198209072005011001



**KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

Alamat: JL. Daeng Tata Raya Parangtambung Makassar 90224
Telp. 0411-864935, Fax. 0411-861507, HP. 0853-1122-4040, Email: jtk@unm.ac.id | laman tik @ unm.ac.id

**LEMBAR PENGESAHAN
PROPOSAL PENELITIAN**

Yang bertanda tangan di bawah ini, dengan ini menerangkan bahwa mahasiswa tersebut di bawah ini:

Nama : SUCI RAHMADANY
NIM : 1929140013
Program Studi : Teknik Komputer - (S1)
Jurusan : Teknik Informatika dan Komputer
Judul : Analisis Keamanan Jaringan pada Fasilitas Internet (Wi-Fi SSID SSO_UNM_Backup) Terhadap Serangan Packet Sniffing di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar

Setelah laporan proposal yang disusun oleh mahasiswa tersebut kami periksa, maka dinyatakan memenuhi syarat untuk melaksanakan **seminar proposal penelitian**.

Pembimbing I,

Dr. Mustari S. Lamada, S.Pd. M.T.
NIP. 19750505 200501 1 001

Makassar, 6 Maret 2023

Pembimbing II,

Dr. Lendra Jaya, S.Pd., M.T
NIP. 198209072005011001

Mengetahui,

Dr. Mustari S. Lamada, S.Pd. M.T.
NIP. 19750505 200501 1 001

Ketua Program Studi
Teknik Komputer - (S1)

Dr. Satria Gunawan Zain, S.Pd., M.T
NIP. 19800809 201012 1 002





**KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

Alamat: Jl. Daeng Tata Raya Paranglambung Makassar – 90224
Telp. 0411-864935, Fax. 0411 – 861507, IIP. 0853-1122-4040, Email: jtik@unm.ac.id | Laman.tik.ft.unm.ac.id

Makassar, 30 September 2023

Nomor : 425/UN36.2/JTIK/III/2023
Sifat : Penting
Lampiran : 1 (satu) Eksamplar
Hal : Undangan Seminar Proposal

Kepada Yth :

1. Ketua Jurusan Teknik Informatika dan Komputer
 2. Sekretaris Jurusan Teknik Informatika dan Komputer
 3. Ketua Prodi Pendidikan Teknik Informatika dan Komputer (S1)
 4. Dr. Mustari S. Lamada, S.Pd. M.T. (Pembimbing I)
 5. Dr. Hendra Jaya, M.T. (Pembimbing II)
 6. Muliadi, S.Pd., M.T. (Penguji I)
 7. Alifya NFH, S.Pd., M.Pd. (Penguji II)
- di Makassar

Dengan Hormat,

Berdasarkan permohonan mahasiswa yang telah memenuhi persyaratan administrasi untuk mengikuti **Seminar Proposal Penelitian**, maka kepada Bapak/Ibu dimohon kesediaannya untuk mengikuti dan menguji mahasiswa tersebut namanya di bawah:

Nama : SUCI RAHMADANY
NIM : 1929140013
Program Studi : Teknik Komputer - (S1)
Judul : Analisis Keamanan Jaringan pada Fasilitas Internet (Wi-Fi SSO UNM) Terhadap Serangan Packet Sniffing di Fakultas Teknik Universitas Negeri Makassar
Hari/Tanggal : Rabu/ 29 Maret 2023
Waktu : 13.30 - 15.30 WITA
Media/Tempat : Join Zoom Meeting
<https://us06web.zoom.us/j/2405753575?pwd=T2o0akVXZ0s1bEhzWkVENXl3ZFBrdz09>

Meeting ID: 240 575 3575
Passcode: TIKFTUNM

Demikian undangan ini disampaikan, atas kehadiran Bapak/Ibu diucapkan terima kasih.

Ketua Jurusan,
Teknik Informatika dan Komputer



Dr. Ir. Mustari S. Lamada, S.Pd. M.T.
NIP 19750505 200501 1 001



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

Alamat: Jl. Daeng Tata Raya Parangtambung Makassar – 90224
 Telp. 0411-864935, Fax. 0411 – 861507, HP. 0853-1122-4040, Email: juk@unm.ac.id | Laman tik.ft.unm.ac.id

LEMBAR PENGESAHAN
REVISI PROPOSAL PENELITIAN

Yang bertanda tangan di bawah ini, dengan ini menerangkan bahwa mahasiswa tersebut di bawah ini:

Nama : Suci Rahmahdany
 NIM : 1929140013
 Program Studi : Teknik Komputer
 Jurusan : Teknik Informatika dan Komputer
 Judul : Analisis Keamanan Web Pada Fasilitas Internet Terhadap Serangan Packet Sniffing Di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar.

Setelah proposal penelitian yang disusun oleh mahasiswa tersebut kami periksa, maka dinyatakan memenuhi syarat untuk melaksanakan **penelitian**.

Makassar, 18 April 2023

Pembimbing I,

Dr. Mustari S. Lamada, S.Pd. M.T.
 NIP 19750505 200501 1 001

Pembimbing II,

Dr. Hendra Jaya, S.Pd., M.T
 NIP. 198209072005011001

Penanggap I,

Dr. Muliadi, S.Pd., M.T.
 NIP 19741116 200112 1 001

Penanggap II,

Alifia Nfh, S.Pd., M.Pd
 NIP 19920401 201803 2 001

Mengetahui:

Ketua Jurusan
 Teknik Informatika dan Komputer

Dr. Mustari Lamada, M.T.
 NIP 19750505 200501 1 001

Ketua Program Studi
 Teknik Komputer – (S1)

Dr. Satria Gunawan Zain, S.Pd., M.T
 NIP. 19800809 201012 1 002



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR (UNM)
FAKULTAS TEKNIK

Alamat: Jalan Daeng Tata Raya Paranglambung Makassar
Telp (0411) 865677 Fax. (0411) 861377
Laman: www.unm.ac.id

Nomor : 2646/UN36.2/PP/2023
Lampiran : 1 (satu) berkas
Hal : **Permintaan Izin Penelitian**

14 Agustus 2023

Yth,
Ketua Jurusan Teknik Informatika dan Komputer
di-
Makassar

Disampaikan bahwa mahasiswa tersebut di bawah ini:

Nama : **Suci Rahmadany**
NIM : 1929140013
Program Studi : Teknik Komputer - S1

Akan mengadakan penelitian dalam rangka penulisan Skripsi yang berjudul:

"Analisis Keamanan Website terhadap Serangan Packet Sniffing di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar"

Penelitian yang dimaksud direncanakan berlangsung selama kurang lebih 3 (Tiga) bulan dibawah koordinasi dosen pembimbing:

Dr. Ir. Mustari S. Lamada, S.Pd., M.T.
197505052005011001

Dr. Hendra Jaya, S.Pd., M.T.
198209072005011001

Schubungan dengan judul tersebut di atas, maka kami mohon kiranya mahasiswa yang bersangkutan dapat diizinkan melakukan penelitian di **Laboratorium Jaringan TIK** guna penulisan Skripsi.

Demikian penyampaian kami, atas perkenaan Bapak/Ibu diucapkan terima kasih.

Makassar, 14 Agustus 2023
a.n Dekan
Wakil Dekan Bidang Akademik



Prof. Dr. Drs. Ir. Jamaluddin P, MP., IPM.
NIP. 196707231992031002



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR (UNM)

FAKULTAS TEKNIK
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

Alamat: Jalan Daeng Tata Raya Parangtambung Makassar

Telp (0411) 865677 – Fax. (0411) 861377

Laman: jtik.ft.unm.ac.id

SURAT KETERANGAN

No: 2247/UN36.2/JTIK/IX/2023

Yang bertanda tangan dibawah ini:

Nama : Dr. Ir. Mustari S. Lamada, S.Pd., M.T.

NIP : 197505052005011001

Jabatan : Ketua Jurusan TIK

Menerangkan bahwa, mahasiswa berikut:

Nama : Suci Rahmadany

NIM : 1929140013

Program Studi : Teknik Komputer - SI

Telah selesai melaksanakan penelitian Skripsi yang berjudul **Analisis Keamanan Website terhadap Serangan Packet Sniffing di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar** yang dilaksanakan pada Laboratorium Jaringan TIK.

Demikian penyampaian kami, atas kerjasamanya kami ucapkan banyak terima kasih.

Makassar, 25 September 2023

Ketua Jurusan TIK

Dr. Ir. Mustari S. Lamada, S.Pd., M.T.

NIP. 197505052005011001



**KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK**

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

Alamat: Jl. Daeng Tata Raya Parangtambung Makassar – 90224

Telp. 0411-864935, Fax. 0411 – 861507, HP. 0853-1122-4040, Email: jtik@unm.ac.id | Laman tik.ft.unm.ac.id

LEMBAR KONSULTASI PROPOSAL

Nama : Suei Rahmadany
NIM : 1929140013
Prodi : Teknik Komputer
Judul : Analisis Keamanan Website Terhadap Serangan Packet Sniffing di Jurusan Teknik Informatika dan Komputer Fakultas Teknik UNM

Pembimbing I : **Dr. Mustari S.Lamada, S.Pd., M.T**
Pembimbing II : Dr. Hendra Jaya, M.T

No	Tanggal	Keterangan	Paraf
1.	31 Agustus 2023	<ul style="list-style-type: none"> Ceklel keamanan website Salah satu user coba login beberapa user Dilakukan cara kerja Packet Sniffing Kuasai jenis-jenis tools yg digunakan 	
2	31 / September 2023	<ul style="list-style-type: none"> Konsultasi dengan dosen mengenai skripsi Perbaikan skripsi mengenai Tata tertib 	

3-26 / September - 2023

Pembimbing I

Dr. Mustari S.Lamada, S.Pd., M.T
NIP. 197505052005011001



KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER



Alamat: Jl. Daeng Tata Raya Parangtambung Makassar – 90224

Telp. 0411-864935, Fax. 0411 861507, HP. 0853-1122-4040, Email: jtik@unm.ac.id | Laman tik.ft.unm.ac.id

LEMBAR KONSULTASI HASIL PENELITIAN

Nama : Suci Rahmahdany
NIM : 1979140013
Jurusan / Prodi : Teknik Komputer
Judul : Analisis Keamanan *Website* Terhadap Serangan *Packet Sniffing* Di Jurusan Teknik Informatika dan Komputer Fakultas Teknik UNM

Pembimbing I : Dr. Mustari S.Lamada, S.Pd., M.T
Pembimbing II : Dr. Hendra Jaya, S.Pd., M.T

No	Tanggal	Keterangan	Paraf
1.	22/09-23	- Perbaiki gambar - perus- - asy d. mrgu.	
2	29/09-28	Ace Am	

Pembimbing II



Dr. Hendra Jaya, S.Pd., M.T
NIP. 19750505 200501 1 101



**KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

Alamat: Jl. Daeng Tata Raya Parangtambung Makassar -- 90224
Telp. 0411-864935, Fax. 0411 -- 861507, HP. 0853-1122-4040, Email: jtik@unm.ac.id | Laman tik.ft.unm.ac.id

LEMBAR PENGESAHAN HASIL

Yang bertanda tangan di bawah ini, dengan ini menerangkan bahwa mahasiswa tersebut di bawah ini:

Nama : SUCI RAHMADANY
NIM : 1929140013
Program Studi : Teknik Komputer - (S1)
Jurusan : Teknik Informatika dan Komputer
Judul : Analisis Keamanan Web Terhadap Serangan Packet Sniffing di
Jurusan Teknik Informatika dan Komputer Universitas Negeri
Makassar

Setelah laporan hasil yang disusun oleh mahasiswa tersebut kami periksa, maka dinyatakan memenuhi syarat untuk melaksanakan **seminar hasil penelitian**.

Pembimbing I,

Dr. Mustari S. Lamada, S.Pd. M.T.
NIP. 19750505 200501 1 001

Makassar, 23 September 2023

Pembimbing II,

Dr. Hendra Jays, S.Pd. M.T.
NIP. 19750505 200501 1 101

Mengetahui,

Ketua Jurusan

Teknik Informatika dan Komputer

Dr. Mustari S. Lamada, S.Pd. M.T.
NIP. 19750505 200501 1 001

Ketua Program Studi

Teknik Komputer - (S1)

Dr. Satria Gunawan Zain, S.Pd., M.T
NIP. 19800809 201012 1 002





**KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

Alamat: Jl. Daeng Tata Raya Parangtambung Makassar 90224
Telp. 0411-864935, Fax. 0411-861507, HP. 0853-1122-4040, Email: jtik@unm.ac.id | Laman.tik.ft.unm.ac.id

Makassar, 30 September 2023

Nomor : 2296/UN36.2/JTIK/IX/2023
Sifat : Penting
Lampiran : 1 (satu) Eksamplar
Hal : Undangan Seminar Hasil

Kepada Yth :

1. Ketua Jurusan Teknik Informatika dan Komputer
 2. Sekretaris Jurusan Teknik Informatika dan Komputer
 3. Ketua Prodi Pendidikan Teknik Informatika dan Komputer (S1)
 4. Dr. Ir. Mustari S. Lamada, S.Pd. M.T. (Pembimbing I)
 5. Dr. Hendra Jaya, M.T. (Pembimbing II)
 6. Dr. Muliadi, S.Pd., M.T. (Penguji I)
 7. Alifya NFH, S.Pd., M.Pd. (Penguji II)
- di Makassar

Dengan Hormat,

Berdasarkan permohonan mahasiswa yang telah memenuhi persyaratan administrasi untuk mengikuti **Seminar Hasil Penelitian**, maka kepada Bapak/Ibu dimohon kesediaannya untuk mengikuti dan menguji mahasiswa tersebut namanya di bawah:

Nama : SUCI RAHMADANY
NIM : 1929140013
Program Studi : Teknik Komputer - (S1)
Judul : Analisis Keamanan Web Terhadap Serangan Packet Sniffing di Jurusan Teknik Informatika dan Komputer Universitas Negeri Makassar
Hari/Tanggal : Senin/ 02 Oktober 2023
Waktu : 13.30 - 15.30 WITA
Media/Tempat : Join Zoom Meeting
<https://us06web.zoom.us/j/2405753575?pwd=T2o0akVXZ0s1bEhzWkVENXl3ZFBrdz09>

Meeting ID: 240 575 3575
Passcode: TIKFTUNM

Demikian undangan ini disampaikan, atas kehadiran Bapak/Ibu diucapkan terima kasih.

Ketua Jurusan,
Teknik Informatika dan Komputer



Dr. Ir. Mustari S. Lamada, S.Pd. M.T.
NIP 19750505 200501 1 001



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS NEGERI MAKASSAR
FAKULTAS TEKNIK

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

Alamat: Jl. Daeng Tata Raya Parangtambung Makassar 90224

Telp. 0411-861935, Fax. 0411-861507, HP. 0853-1122-4040, Email: jtk@unm.ac.id | Laman: jtk.unm.ac.id

**LEMBAR PENGESAHAN
REVISI HASIL PENELITIAN**

Yang bertanda tangan di bawah ini, dengan ini menerangkan bahwa mahasiswa tersebut di bawah ini:

Nama : Suci Rahmahdany
NIM : 1929140013
Program Studi : Teknik Komputer – (S1)
Jurusan : Teknik Informatika dan Komputer
Judul : Analisis Keamanan *Website* Terhadap Serangan *Packet Sniffing* di Jurusan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Makassar

Setelah revisi laporan penelitian yang disusun oleh mahasiswa tersebut kami periksa, maka dinyatakan memenuhi syarat untuk melaksanakan **ujian skripsi**.

Makassar, 03 Oktober 2023

Pembimbing I,

Dr. Mustari S. Lamada, S.Pd., M.T.
NIP. 19750505 200501 1 001

Pembimbing II,

Prof. Dr. Hendra Jaya, S.Pd., M.T.
NIP. 19820907 200501 1 001

Penanggap I,

Dr. Muliadi, S.Pd., M.T.
NIP. 19741116 200112 1 001

Penanggap II,

Alifya Nfh, S.Pd., M.Pd
NIP. 19920401 201803 2 001

Mengetahui:

Ketua Program Studi
Teknik Komputer

Dr. Satria Gunawan Zain, S.Pd., M.T.
NIP. 19800809 201012 1 002



Ketua Jurusan

Teknik Informatika dan Komputer

Dr. Mustari Lamada, M.T.
NIP. 19750505 200501 1 001

RIWAYAT HIDUP



Suci Rahmahdany, lahir pada tanggal 08 Desember 2000 hari Rabu di Kota Makassar, Provinsi Sulawesi Selatan. Anak ke 9 dari 10 bersaudara dari pasangan Ayub, S. Sos., dan Sri Wanti Hasnia. Penulis menempuh Pendidikan Sekolah Dasar di SD

Inpres Tamalanrea 6 pada tahun 2012. Kemudian melanjutkan Pendidikan pada Sekolah Menengah Pertama (SMP) di SMP Negeri 30 Makassar yang terletak di Perumahan Bumi Tamalanrea Permai (BTP) dan tamat pada tahun 2016. Kemudian melanjutkan Pendidikan pada Sekolah Menengah Atas (SMA) di SMA Negeri 1 Gowa dan tamat pada tahun 2019. Pada tahun 2019, penulis melanjutkan Pendidikan ke jenjang Strata 1 di Universitas Negeri Makassar tepatnya di Fakultas Teknik, Jurusan Teknik Informatika dan Komputer, Program Studi Teknik Komputer melalui jalur SNMPTN.