ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

TUGAS AKHIR

Disusun Untuk Memenuhi Syarat Kelulusan Program Strata 1 pada
Sekolah Tinggi Manajemen Informatika dan Komputer
(STMIK) Palangkaraya

OLEH:

LIANTONI
NIM C1957201023
PROGRAM STUDI SISTEM INFORMASI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
2022

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

TUGAS AKHIR

Disusun Untuk Memenuhi Syarat Kelulusan Program Strata 1 pada
Sekolah Tinggi Manajemen Informatika dan Komputer
(STMIK) Palangkaraya

OLEH:

LIANTONI
NIM C1957201023
PROGRAM STUDI SISTEM INFORMASI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
2022

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama Mahasiswa : **LIANTONI**
N I M : C1957201023

menyatakan bahwa Tugas Akhir dengan judul:

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Adalah hasil karya saya dan bukan merupakan duplikasi sebagian atau seluruhnya dari karya orang lain, kecuali bagian yang sumber informasi dicantumkan.

Pernyataan ini dibuat dengan sebenar-benarnya secara sadar dan bertanggung jawab dan saya bersedia menerima sanksi pembatalan tugas akhir apabila terbukti melakukan duplikasi terhadap tugas akhir atau karya ilmiah lain yang sudah ada.

Palangka Raya, 28 Mei 2022
Yang Membuat Pernyataan,

LIANTONI

iii

PERSETUJUAN

ANALISIS KEAMANAN JARINGAN PUBLIK PADA
FASILITAS SOSIAL DI KOTA PALANGKA RAYA
MENGGUNAKAN WIRESHARK

Tugas Akhir ini telah disetujui untuk diuji
pada Tanggal 28 Mei 2022

Pembimbing I,

Sam'ani, ST., M.Kom.
NIK. 197703252005105

Pembimbing II,

Hafiz Riyadli, M.Kom.
NIK. 198604042010103

Mengetahui :
Ketua STMIK Palangkaraya,

Suparno,M.Kom
NIK. 196901041995105

iv

PENGESAHAN

ANALISIS KEAMANAN JARINGAN PUBLIK PADA
FASILITAS SOSIAL DI KOTA PALANGKA RAYA
MENGGUNAKAN WIRESHARK

Tugas Akhir ini telah Diuji, Dinilai dan Disahkan
Oleh Tim Penguji pada Tanggal 28 Mei 2022

Tim Penguji :

1. Ferdiyani Haris, M. Kom. .....
   Sebagai Ketua

2. Norhayati, M. Pd. .....
   Sebagai Sekretaris

3. Deden Andriawan, M.Kom. .....
   Sebagai Anggota

4. Sam'ani, S. T., M. Kom. .....
   Sebagai Anggota

5. Hafiz Riyadli, M. Kom. .....
   Sebagai Anggota

v

MOTTO DAN PERSEMBAHAN

"Kesuksesan bukan tentang seberapa banyak uang yang kamu hasilkan bisa membawa manfaat dan perubahan untuk lingkungan kamu dan hidup orang lain"

Kupersembahkan untuk :

- Kedua orang tua-ku yang tercinta,

  Kakak-ku, serta keluaga besar-ku yang tersayang, terimakasih telah memberikan banyak dukungan, nasihat serta doa kepada ku.
- Bapak dan Ibu Dosen STMIK Palangkaraya, terimakasih Banyak untuk semua ilmu, didikan dan pengalaman yang Sangat berarti yang telah kalian berikan kepada kami.
- Teman- teman angkatan 2019 yang selalu memberi semangat.

INTISARI

Liantoni, C1955201023, 2022. *Analisis Keamanan Jaringan Publik Pada Fasilitas Sosial Di Kota Palangka Raya Menggunakan Wireshark*, Pembimbing I Sam'ani, ST., M.Kom., Pembimbing II, Hafiz Riyadi, M.Kom

Dinas Komunikasi, Informatika Persandian dan Statistik Kota Palangka Raya telah menerapkan jaringan wifi gratis di beberapa fasilitas umum Kota Palangka Raya. Pada saat ini issue keamanan jaringan menjadi sangat penting dan patut untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para hacker, baik jaringan wired LAN maupun wireless LAN. Pada saat data dikirimkan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk melakukan penyadapan atau mengubah data tersebut

Metode analisis yang digunakan dalam perancangan dan pembangunan aplikasi ini adalah Analisis *PIECES*, Teknik pengumpulan data yang digunakan dalam penelitian ini yaitu observasi, wawancara, penelitian pustaka, kuesioner dan dokumentasi, tahapan yang digunakan dalam penelitian ini adalah *Deskriptif kualitatif* selanjutnya akan dilakukan evaluasi dengan cara ujicoba sistem dengan menggunakan *Wireshark* Testing untuk menguji sistem apakah memiliki jaringan yang bisa di ekploitasi atau tidak, hasil dari penelitian ini . Untuk sistem keamanan jaringan menggunakan WEP memiliki teknik enkripsi yang sangat rentan dan Sistem keamanan ini akan mempermudah bagi administrator dalam memantau client dan menganalisa setiap gangguan yang muncul.

Berdasarkan hasil kuesioner yang telah disebarkan ke lima belas responden menyatakan "Sangat Setuju" bahwa penelitian ini bisa di pertimbangakan sebagai bahan evaluasi keaamanan sistem pada Taman Pasuk Kameloh dengan presentase sebesar 94% hasil tersebut maka dapat dikatakan tanggapan dari semua responden adalah sangat baik.

Kata Kunci: Jaringan Publik, *Wifi, Wireshark, Wireless Access Point*

ABSTRAK

Liantoni, C1955201023, 2022. *Analysis of Public Network Security in Social Facilities in Palangka Raya City Using Wireshark*, Supervisor I Sam'ani, ST., M.Kom., Supervisor II, Hafiz Riyadi, M.Kom

The Office of Communication, Informatics, Encoding and Statistics of the City of Palangka Raya has implemented a free wifi network in several public facilities of the City of Palangka Raya. At this time the issue of network security becomes very important and deserves attention, networks connected to the internet are basically insecure and can always be exploited by hackers, both wired LAN and wireless LAN networks. When data is sent through several terminals to reach its destination, it means that it will provide an opportunity for other users who are not responsible for tapping or changing the data.

The analytical method used in the design and development of this application is PIECES analysis. The data collection techniques used in this study are observation, interviews, library research, questionnaires and documentation. system using Wireshark Testing to test the system whether it has a network that can be exploited or not, the results of this study. For network security systems using WEP, encryption techniques are very vulnerable and this security system will make it easier for administrators to monitor clients and analyze any disturbances that arise.

Based on the results of the questionnaire that has been distributed to fifteen respondents stating "Strongly Agree" that this research can be considered as material for evaluating the security of the system at Taman Pasuk Kameloh with a percentage of 94% of these results, it can be said that the responses from all respondents are very good.

Keywords: *Public Network, Wifi, Wireshark, Wireless Access Point*

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiratan Tuhan Yang Maha Esa yang telah memberikan suka cita serta kekuatan sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul "Analisis Keamanan Jaringan Publik Pada Fasilitas Sosial Di Kota Palangka Raya Menggunakan Wireshark" terwujudnya Tugas Akhir ini tidak lepas dari bantuan berbagai pihak yang telah mendorong dan membimbing penulis, baik tenaga, ide-ide, maupun pemikiran. Adapun tujuan penulisan Tugas Akhir ini adalah untuk memenuhi salah satu syarat penulisan Tugas Akhir pada Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya. Pada Kesempatan ini penulisan juga ingin menyampikan ucapan teriama kasih kepada.

1. Suparno,M.Kom selaku Ketua Sekolah Tinggi Manajemen Informatika dan komputer (STMIK) Palangkaraya.
2. Dra. Fifi Arfiana , Msi Selaku Kepala Dinas Diskominfo Kota Palangkaraya dan Maharani Selaku Penanggung Jawab Humas Diskomifo Kota Palangkaraya yang telah memberikan waktu dan tempat untuk melakukan penelitian.
3. Sam'ani, ST., M.Kom selaku dosen pembimbing I yang telah membimbing dalam materi topik penelitian secara keseluruhan.
4. Hafiz Riyadli, M.Kom selaku dosen pembimbing II yang telah membimbing dalam materi penulisan secara keseluruhan.
5. Yang sangat istimewa orang tua dan keluarga penulis yang selalu memberi dukungan semangat yang tidak henti-hentinya kepada penulis di dalam proses penulisan Tugas Akhir yang penulis tempuh sekarang.

6. Seluruh teman-teman seperjuangan dan sepenanggungan di Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya yang selalu memberikan dukungan semangat baik secara langsung maupun tidak langsung.

Penulis menyadari bahwa tak ada gading yang tak retak, begitu juga dengan Tugas Akhir ini yang tidak luput dari kekurangan.

Palangka Raya, 28 Mei 2022

Penulis,

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

A. Latar Belakang

Seiring dengan perkembangan teknologi pada era sekarang internet merupakan hal yang sangat dibutuhkan oleh semua aspek kehidupan manusia, karena dengan internet kita bisa dengan mudah berkomunikasi dengan orang-orang yang berada jauh sampai keluar negeri melalui media sosial yang telah banyak disediakan sekarang, tidak hanya sebagai media komunikasi tetapi juga sebagai salah satu tempat mengekspresikan diri, dan internet juga dapat digunakan sebagai media untuk menyimpan data-data yang penting.

Untuk bisa terhubung ke dalam sebuah internet kita bisa menggunakan kabel ataupun wireless (*Wifi*), seperti yang kita ketahui seseorang bisa terkoneksi ke sebuah intenet kapanpun dan dimanapun selagi terdapat jaringan melalui media seperti komputer, laptop, tablet, notebook, ataupun smartphone.

Pada saat ini *issue* keamanan jaringan menjadi sangat penting dan patut untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh para hacker, baik jaringan *wired LAN (Local Area Network)* maupun *wireless LAN (Local Area Network)*. Pada saat data dikirimkan melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada pengguna lain yang tidak bertanggung jawab untuk melakukan penyadapan atau mengubah data tersebut.

Dalam pembangunan perancangannya, sistem keamanan jaringan yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya Serangan *ARP (Address Resolution Protocol) Spoofing* merupakan serangan yang berbahaya karena dapat mendukung terjadinya serangan jaringan komputer lainnya seperti *Denial of Service, Man in the middle attack, host impersonating* dan lain-lain.

Dinas Komunikasi, Informatika Persandian dan Statistik Kota Palangka Raya telah menerapkan jaringan wireless (*Wifi*), gratis di beberapa fasilitas umum Kota Palangka Raya. Terdapat ada 5 jaringan yang terpasang pada tempat umum inilah yang sering rentan dari para hacker. Banyak pengguna jaringan wireless (*Wifi*), tidak bisa membayangkan jenis bahaya apa yang sedang menghampiri mereka pada saat sedang berasosiasi dengan *wireless access point* (*WPA*).

Berdasarkan latar belakang yang diuraikan diatas, maka peneliti tertarik untuk menganalisis suatu jaringan wireless (*Wifi*), yang ada pada fasilitas umum di Kota Palangka Raya dan mengangkat judul "Analisis Keamanan Jaringan Publik Pada Fasilitas Sosial Di Kota Palangka Raya Menggunakan Wireshark*"*.

B. Rumusan Masalah

Pada penelitian ini terdapat rumusan permasalahan yang menjadi titik utama yaitu bagaimana cara mengalisis keamanan jaringan publik pada fasilitas sosial di kota palangka raya menggunakan *wireshark* ?

C. Batasan Masalah

Adapun Batasan masalah dari penelitian ini supaya tidak terjadi kesalahan persepsi dan tidak meluaskan pokok bahasan yaitu.

1. Melakukan pengujian penetrasi pada *wifi* menggunakan tools *Wireshark* sehingga dapat menemukan celah yang tampak dari wifi tersebut
2. Penelitian ini tidak melakukan implementasi peningkatan keamanan jaringan yang sudah ada dan hanya memberikan cara yang tepat yang sebaiknya dilakukan untuk mengantisipasi dari terjadinya serangan *sniffing* (Pencurian Data) pada jaringan *Wifi.*
3. Adapun lokasi yang di analisis antara lain jaringan *wifi*.id non-berbayar pada taman Pasuk Kameloh Kota Palangka Raya.

D. Tujuan dan Manfaat

Adapun Tujuan dan Manfaat pada penelitian ini adalah :

1. Tujuan

   Tujuan dari pemilihan judul ini yaitu agar hasil dari penelitian yang dilakukan akan memberikan cara yang tepat untuk dapat mencegah terjadinya penyerangan *sniffing* saat mengakses jaringan bebas atau terbuka pada fasilitas umum.

2. Manfaat

   a. Manfaat bagi masyarakat STMIK Palangka Raya

Penelitian ini diharapkan dapat berguna bagi peneliti lainnya agar dapat di lanjutkan dan di kembangkan arah penelitian ini agar dapat lebih kritisi dalam menganalisis jaringan terbuka pada fasilitas umum lainnya

b. Manfaat bagi masyarakat luas

Penelitian ini di harapkan agar masyarakat luas dapat mengerti tentang keamanan jaringan yang ada pada fasilitas umum sehingga terhindar dari segala macam pencurian data pribadi pada *device* nya saat mengakses jaringan terbuka.

E. Jenis Penelitian

Dalam suatu penelitian seorang peneliti harus menggunakan jenis penelitian yang tepat. Hal ini dimaksud agar peneliti dapat memperoleh gambaran yang jelas mengenai masalah yang dihadapi serta langkah-langkah yang digunakan dalam mengatasi masalah tersebut.

Adapun jenis penelitian yang digunakan dalam penelitian ini adalah menggunakan metode penelitian Deskriptif kualitatif.

F. Sistematika Penulisan

Penulis memberikan gambaran terhadap pembahasan Laporan Tugas Akhir ini agar sesuai dengan tujuan, maka penulisan disusun dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini akan membahas mengenai latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat, sistematika penulisan, dan penjelasan istilah kunci.

BAB II LANDASAN TEORI

Bab ini menguraikan secara singkat mengenai dasar teori-teori yang berkaitan dengan judul laporan analisis ini dan Penelitian yang relevan.

BAB III METODE PENELITIAN

Bab ini akan membahas tentang metode pengumpulan data, metode pengembangan sistem, tinjauan umum, analisis dan hasil penelitian.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini menjelaskan implementasi program, serta hasil penelitian dan pembahasan secara detail yang ada di bab sebelum nya. Bab ini merupakan bagian yang penting dari penelitian karena bagian ini memuat semua temuan ilmiah yang diperoleh sebagai hasil penelitian, diantaranya hasil analisis, pengujian, hasil uji coba, dan hasil penelitian dan pembahasan. Hasil penelitian dan pembahasan menguraikan pembahasan tentang analisis yang diteliti oleh penulis.

BAB V PENUTUP

Bab ini memuat kesimpulan dan saran-saran penulis dari penulisan yang telah dibahas.

G. Penjelasan Istilah Kunci

1. Jaringan Publik adalah jaringan yang dibangun oleh pemerintah maupun penyedia jasa telekomunikasi kepada publik, baik yang berorientasi profit maupun non-profit, sehingga masyarakat luas dapat memanfaatkannya dalam bertukar informasi.
2. *Wifi* Kependekan Dari *Wireless Fidelity* Yaitu Sebuah Media Penghantar Komunikasi Data Tanpa Kabel Yang Bisa Digunakan Untuk Komunikasi Atau mentransfer Program Dan Data Dengan Kemampuan Yang Sangat Cepat.
3. *Wireshark* merupakan salah satu tools atau aplikasi capture paket data berbasis *open-source* untuk melakukan analisis dan pemecah masalah jaringan.
4. *Sniffing* adalah tindak kejahatan penyadapan yang dilakukan menggunakan jaringan internet dengan tujuan utama untuk mengambil data dan informasi sensitive secara illegal.
5. *Hacker* adalah istilah untuk seseorang yang mempelajari, memodifikasi, menganalisa dan masuk ke sebuah jaringan komputer.
6. *Wireless Access Point* adalah suatu sistem yang juga dapat diterapkan untuk mengamankan jaringan nirkabel.

BAB II

TINJAUAN PUSTAKA

A. Dasar Teori

1. Teori yang berkaitan dengan topik penelitian

    a. Analisis

Analisis sistem adalah sebuah istilah yang secara kolektif mendeskripsikan fase-fase awal pengembangan sistem, (Muslihudin dan Oktaflianto, 2016:27).

Menurut Yuni (2020) Pengertian analisis yang dikemukakan di atas, dapat disimpulkan bahwa analisis adalah bukan hanya sekedar penelusuran atau penyelelidikan, tetapi suatu kegiatan yang terencana dan dilakukan secara sungguh-sungggguh dengan menggunakan pemikiran yang kritis untuk memperoleh kesimpulan dari apa yang ditaksir.

Pengertian analisis yang dikemukakan di atas, dapat disimpulkan bahwa analisis adalah bukan hanya sekedar penelusuran atau penyelelidikan, tetapi suatu kegiatan yang terencana dan dilakukan secara sungguh-sungggguh dengan menggunakan pemikiran yang kritis untuk memperoleh kesimpulan dari apa yang ditaksir.

b. Jaringan

Menurut Kustanto (2015) " Jaringan komputer adalah kumpulan dua atau lebih komputer yang saling berhubungan satu sama lain untuk melakukan komunikasi data dengan menggunakan protokol komunnikasi melalui media komunikasi (kabel atau nirkabel), sehingga komputer-komputer tersebut dapat saling berbagi informasi, data program-program, dan penggunaan perangkat keras secara bersama". Dalam hal ini komunikasi data yang bisa dilakukan melalui jaringan komputer dapat berupa data teks, gambar, vidio dan suara.

c. Keamanan Jaringan

Menurut Singh (2014), keamanan jaringan adalah melindungi informasi yang ada pada sistem informasi dari orang yang tidak memiliki hak akses atau hak untuk melakukan modifikasi terhadap informasi tersebut baik dari sisi penyimpanan, waktu proses ataupun saat informasi transit di suatu tempat. Keamanan informasi adalah gabungan dari keamanan komputer dan juga keamanan komunikasi. Keamanan informasi bukan hanya keamanan komputer saja. keamanan informasi menyangkut lebih luas dibandingkan keamanan komputer, seperti memberikan keamanan pada informasi aset yang dimiliki dari pencurian ataupun bencana alam dan juga dari social attack engineering seperti seseorang melakukan penipuan kepada target agar dapat memberikan informasi yang sensitif kepadanya. Keamanan informasi adalah suatu proses untuk mengamankan informasi dari yang tidak berhak, menggunakan, merusak, memodifikasi, mendistribusikan informasi tersebut. Proses berulang ini melibatkan latihan terus menerus, penilaian, proteksi, memonitor, mendeteksi, merespon insiden dan memperbaiki, dan juga melakukan dokumentasi dan ulasan. Proses ini membuat keamanan informasi menjadi bagian yang tidak dapat dipisahkan dari segala operasi bisnis di semua kalangan.

d. Fasilitas Publik

Pengertian sarana dan prasarna Menurut Kamus Besar Bahasa Indonesia (KBBI) Sarana adalah segala sesuatu yang dapat dipakai sebagai alat dalam mencapai maksud atau tujuan. Sedangkan prasarana

adalah segala sesuatu yang merupakan penunjang utama terselenggaranya suatu proses (usaha, pembangunan, proyek). untuk lebih memudahkan membedakan keduanya. Sarana lebih ditujukan untuk benda-benda yang bergerak, sedangkan prasarana lebih ditujukan untuk benda-benda yang tidak bergerak seperti bangunan. Definisi fasilitas adalah segala sesuatu yang berbentuk benda maupun uang yang dapat memudahkan serta memperlancar pelaksanaan suatu usaha tertentu.

Menurut Sam (2008) Fasilitas umum adalah sarana yang disediakan untuk kepentingan umum seperti jalan raya, lampu penerangan jalan, halte, trotoar, dan jembatan penyebrangan. Fasilitas yang disediakan ini merupakan sarana yang memberikan kemudahan bagi masyarakat sehingga harus dipelihara dengan baik. Fasilitas pejalan kaki berfungsi memisahkan pejalan kaki dari jalur lalu lintas kendaraan guna menjamin keselamatan pejalan kaki dan kelancaran lalu lintas.

e. IP

Menurut Nisayanto (2016) Internet Protocol (IP) merupakan Seluruh data yang akan dikirim harus dilewatkan dan diolah oleh *protocol* IP dan dikirimkan sebagai datagram IP untuk sampai kesisi penerima. *Protocol* IP tidak menjamin data yang dikirim aman sampai tujuan. IP hanya melakukan cara terbaik untuk menyampaikan datagram yang dikirim ke tujuan, apabila dalam perjalanan terjadi hal-hal yang tidak di inginkan, maka IP hanya memberikan pemberitahuan pada sisi kirim kalau telah

terjadi permasalahan dalam perjalanan pengiriman data ke tujuan *protocol* ICMP.

f. Subnetting

Menurut Nisayanto (2016) Istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada angka biner 32 bit yang digunakan untuk membedakan *network ID* dengan *host ID*, menunjukkan letak suatu *host*, apakah berada di jaringan lokal atau jaringan luar.

g. Jaringan Komputer

Menurut Sofana (2013) jaringan komputer terbgi beberapa jenis jaringan, yang memisahkan berdasarkan area atau skala dan terbagi menjadi tiga bagan. yaitu:

1) LAN (Local Area Network)

Local area network adalah jaringan lokal yang di buat pada area terbatas. Mislkan dalam satu gedung atau satu ruangan. Kadangkala jaringan lokal di sebut juga jaringan personal atau privat. Lan bisa di gunakan pada sekala kecil yang menggunakan resource secara bersama, seperti penggunaan printer bersama, penggunaan media penyimpanan secara bersama, dan sebagainya.

2) MAN

Metropolitan area network menggunakan metode yang sama dengan *LAN* namum daerah cangkupnya lebih luas. Daerah cangkupan *MAN* bisa satu RW, beberapa kantor yang berada dalam satu komplek yang

sama, satu/beberapa desa, satu/beberapa kota. Dapat dikatankan *MAN* pengembangan dari *LAN*

3) WAN

Wide area network cangkupnya lebih luas dari pada MAN. Cangkupan MAN meliputi satu kawasan, satu Negara, satu pulau, bahkan satu dunia, metode yang digunakan WAN sama seperti yang di gunakan LAN dan MAN. Umumnya WAN di hubungkan dengan jaringan telepon digita. Namun media transmisi lain pun dapat digunakan.

h. Wireless LAN

Menurut Sofana (2013:4) penggunaan peralatan wireless yang berkualitas dan mampu bekerja nonstop, sehingga dapat digunakan kapan saja saat diperlukan. Ada baiknya jika didukung oleh layanan purnajual dari vendor pembuat produk. Kedua teknologi yang digolongkan kedalam jaringan WPAN (Wireless Personal Area Network) ini mempunyai ke unggulan masing-masing. Bluetooth yang tampaknya sangat unggul dalam segala sisi ternyata lebih rawan terhadap interfrensi sedangkan IrDa hampir tidak pengaruh oleh hiruk pikuk frekuensi yang ada di sekitarnya sehingga sangat cocok di gunakan di dalam lingkungan yang penuh dengan frekuensi pengganggu.

i. Wimax

Menurut Nasir (2013) WiMAX adalah singkatan dari Worldwide Interoperability for Microwave Access, merupakan teknologi akses

nirkabel pita lebar (broadband wireless access atau disingkat BWA) yang memiliki kecepatan akses yang tinggi dengan jangkauan yang luas. WiMAX merupakan evolusi dari teknologi BWA sebelumnya dengan fitur-fitur yang lebih menarik. Disamping kecepatan data yang tinggi mampu diberikan, WiMAX juga merupakan teknologi dengan open standar. Dalam arti komunikasi perangkat WiMAX di antara beberapa vendor yang berbeda tetap dapat dilakukan (tidak proprietary). Dengan kecepatan data yang besar (sampai 70 MBps), WiMAX dapat diaplikasikan untuk koneksi broadband 'last mile', ataupun backhaul.

j. Proxy

Menurut Imam (2014) Proxy merupakan server yang berfungsi sebagai perantara antara komputer client dengan server lainya. Server proxy akan meneruskan permintaan atas nama client ke server lain dan menerima respons dari server tersebut untuk kemudian meneruskannya kembali ke komputer client". Dalam menjalankan tugasnya proxy server tidak terlihat oleh komputer client, sebagai contoh saat seorang pengguna yang berinteraksi dengan internet melalui sebuah proxy server tidak akan mengetahui bahwa sebuah proxy server sedang menangani request yang dilakukannya. Web server yang menerima request dari Proxy server akan menginterpresentasikan request-request tersebut seolah-olah datang secara langsung dari komputer client, bukan dari proxy server.

k. Router Modem

Menurut Kustanto dan Saputro (2015) modem “perangkat modulator de modulator yaitu untuk mengubah informasi data digital ke analog atau sebaliknya”. Modem (Modulator Demodulator) berfungsi sebagai media untuk pengiriman data pada jarak jauh atau data pada jaringan global. Proses pengiriman data dilakukan secara serial dalam bentuk pulsa analog frekuensi tinggi dengan prinsip dasar modulasi. Untuk pengiriman jarak jauh digunakan sinyal analog mengingat sinyal digital mempunyai jarak jangkau yang pendek sebagai akibat pengaruh redaman maupun derau pada media pengirimannya, sedangkan pada sinyal analog meskipun mempunyai kelemahan yakni terpengaruh oleh derau selama pengiriman tetapi hal ini dapat diatasi dengan pengiriman pada frekuensi tinggi.

l. Wireshark

Menurut Nisayanto (2016) *Wireshark* merupakan salah satu tool aplikasi *Network Analyzer* atau analisa jaringan *open source*. Awalnya *tool* ini bernama *Ethereal*, pada Mei 2006 proyek ini berganti nama menjadi *Wireshark* karena masalah merek dagang. Penganalisaan kinerja jaringan itu dapat melingkupi berbagai hal, mulai dari proses menangkap pakrt-paket data atau informasi yang belalu-lalang dalam jaringan, sampai digunakan pula untuk *sniffing*, *sniffing* yaitu memperoleh informasi penting seperti *password*, *email*, data sensitif, dan lain-lain. Tampilan

wireshark ini sangat bersahabat karena mengguunakan tampilan grafis atau *GUI.*

Fungsi *Wireshark* antara lain berikut dibawah ini.

1) Menganalisa jaringan.
2) Menangkap paket data atau informasi yang berkeliaran dalam jaringan yang terlihat.
3) Penganalisaan informasi yang didapat dengan melakukan sniffing.
4) Membaca data secara langsung dari Ethernet, Token-Ring, FDDI, Serial (PPP dan SLIP), 802.11 wireless LAN, dan koneksi ATM.
5) Menganalisa transmisi paket data dalam jaringan, proses koneksi dan transmisi data antar komputer.

m. Skala Lickert

Menurut Sugiyono (2015:134), Skala *Likert* digunakan untuk mengukur sikap, pendapat dan persepsi seseorang atau sekelompok orang tentang fenomena item. Untuk setiap pilihan jawaban diberi skor, maka responden harus menggambarkan dan mendukung pernyataan. Untuk digunakan jawaban yang dipilih. Dengan skala *likert*, maka variable yang akan diukur dijabarkan menjadi indikator variable. Kemudian indikator tersebut dijadikan sebagai titik tolak ukur menyusun item-item bite minimal yang dapat berupa pertanyaan dan pernyataan.

Dengan menggunakan Skala Likert, variabel yang akan diukur dijabarkan menjadi dimensi, lalu dijabarkan menjadi subvariabel dan subvariabel dijabarkan lagi menjadi indikator yang dapat diukur.

Akhirnya, indikator-indikator yang terukur dapat menjadi titik tolak untuk membuat item instrument berupa pernyataan atau pertanyaan yang perlu dijawab oleh responden. Setiap jawaban dihubungkan dengan bentuk pernyataan atau dukungan sikap yang diungkapkan dengan kata-kata sebagai berikut :

Tabel 1. Skala Penilaian Untuk Pernyataan Positif dan Negatif

No.	Keterangan	Skor Positif	Skor Negatif
1	Sangat Setuju (SS)	5	1
2	Setuju (S)	4	2
3	Netral (N)	3	3
4	Tidak Setuju (TS)	2	4
5	Sangat Tidak Setuju (STS)	1	5

B. Penelitian Yang Relevan

Beberapa penelitian yang relevan dengan penelitian ini adalah.

1. Penelitian yang dilakukan oleh Agung Nugroho yang berjudul "Analisa Keamanan Jaringan Wireless Local Area Network Dengan Access Point Tp-Link Wa500g". Hasil penelitian ini menunjukkan bahwa pengujian terhadap keamanan pada jaringan wireless dari sisi keamanan access point, dan access point yang digunakan adalah TPLINK WA500G. Metode konsep yang digunakan adalah wireless hacking, pengujiannya diantaranya meliputi reveal SSID (Service Set Identifier), MAC address spoofing , crack WEP (Wired Equivalent Privacy), crack WPA/WPA2 PSK (Wifi Protected Access Pre-Shared

Key). Persamaan penelitian terdahulu dengan yang penulis teliti adalah terletak pada analisa jaringan wireless. Perbedaannya yaitu penelitian yang dilakukan sebelumnya untuk pengujian terhadap celah keamanan access point TP-LINK WA500G dapat memberikan pemahaman terhadap celah keamanannya dan cara untuk pencegahan wireless hacking sedangkan yang penulis teliti adalah untuk menganalisa keamanan jaringan publik untuk mengatasi kemungkinan masalah yang terjadi pada lalu lintas data menggunakan wireshark.

2. Penelitian yang dilakukan oleh M. R. Kurniawan yang berjudul "Analisis Sistem Keamanan Wireless Local Area Network (Wlan) Pada Proses Tethering". Hasil penelitian ini menunjukkan bahwa segi keamanan komunikasi data pada jaringan tersebut rentan terhadap aktivitas ilegal seperti sniffing dan scanning serta kejahatan lainnya. Persamaan penelitian terdahulu dengan yang penulis teliti adalah terletak pada analisa jaringan wireless (wifi). Perbedaannya yaitu penelitian yang dilakukan sebelumnya meneliti jaringan *tethering* sedangkan penulis meneliti jaringan *wifi* terbuka fasilitas sosial.
3. Penelitian yang dilakukan oleh Gilang Kumala Dewi yang berjudul "Analisa Keamanan Jaringan *Wireless (Wifi)* Di Sekolah Menengah Al Firdaus". Hasil penelitian ini menunjukkan bahwa celah pada keamanan yang diterapakan di jaringan wireless Sekolah Menengah Al Firdaus namun untuk saat ini keamanan yang diterapkan sudah tergolong cukup aman. Karena kebanyakan *access point* yang dipasang

sudah menggunakan keamanan setingkat *WPA/WPA2.(Wi-Fi Protected Access)* Persamaan penelitian terdahulu dengan yang penulis teliti adalah terletak pada analisa jaringan *wireless (wifi)*. Perbedaannya yaitu penelitian yang dilakukan sebelumnya meneliti jaringan sekolah sedangkan penulis meneliti jaringan *wireless (wifi)* fasilitas sosial.

4. Penelitian yang dilakukan oleh Bayu Arie Nugroho yang berjudul "Analisis Keamanan Jaringan Pada Fasilitas Internet *wireless (wifi)* Terhadap Serangan *Packet Sniffing*". Hasil penelitian ini menunjukkan bahwa Jaringan *wireless (wifi)* sangat rentan terhadap ancaman serangan, karena komunikasi yang terjadi bersifat terbuka. Diperlukan *system* pengamanan yang baik untuk dapat menjaga keamanan data pengguna agar terhindar dari serangan yang dilakukan oleh orang–orang yang tidak bertanggung jawab. Penelitian ini membahas evaluasi tingkat keamanan fasilitas *wireless (wifi)* di PT. Angkasa Pura I Bandar Udara Internasional Adi Sumarmo Surakarta dengan menggunakan aplikasi *netstumbler, inSSIDer* dan *ettercap*. Persamaan penelitian terdahulu dengan yang penulis teliti adalah terletak pada analisa jaringan wireless. Perbedaannya yaitu penelitian yang dilakukan sebelumnya meneliti jaringan institusi BUMN sedangkan penulis meneliti jaringan terbuka fasilitas sosial.
5. Penelitian yang dilakukan oleh Ayu Syifa Destiani yang berjudul "Analisis Protokol Keamanan Situ Unpas Dengan Menggunakan

Sslstrip Dan *Wireshark*". Hasil penelitian ini menunjukkan bahwa bahwa segi keamanan komunikasi data pada jaringan tersebut rentan terhadap aktivitas ilegal seperti *sniffing* dan *scanning* serta kejahatan lainnya akibat penggunaan aplikasi *NetCut* oleh pihak yang tidak bertanggung jawab. Persamaan penelitian terdahulu dengan yang penulis teliti adalah terletak pada analisa jaringan *wireless (wifi)*. Perbedaannya yaitu penelitian yang dilakukan sebelumnya meneliti jaringan institusi BUMN sedangkan penulis meneliti jaringan terbuka fasilitas publik.

6. Penelitian yang di lakukan Oleh Aulia Rahmah (STMIK Palangka Raya) dengan judul Analisis Jaringan Wireless Pada Kampus STIE YBPK Palangka Raya, meneliti tentang jaringan serta *Qos (Quality of Service) WLAN (Wireless Local Area Network)* kampus STIE YBPK Palangka Raya. Persamaan dengan penulis ialah meneliti jaringan *wireless (wifi*, sedangkan perbedaan dengan penulis ialah dari objek maupun *tools* yang digunakan.
7. Penelitian yang di lakukan Oleh Rizky Dwi M (STMIK Palangka Raya) dengan judul Analisis Sistem Monitoring Jaringan Pada SMPN 2 Pandih Batu Kabupaten Pulang Pisau Menggunakan *Wireshark*. Persamaan dengan penulis ialah sama menggunakan *tools Wireshark*, sedangakan perbedaanny adalah pada objek dan tipe jaringan yang diteliti oleh penulis.

Kesimpulan : Berdasarkan urutan penelitian yang relevan dapat disimpulkan bahwa penelitian yang dilakukan oleh penulis memiliki kesamaan dengan topik peneliti-peneliti tersebut. Dengan menggunakan metode penelitian yang menyesuaikan dengan objek penelitian.

BAB III

METODE PENELITIAN

A. Metode Penelitian

Metode yang digunakan adalah metode *Deskriptif kualitatif* yaitu menjelaskan tentang keadaan atau situasi yang terjadi. Tahap yang dilakukan adalah menggunakan kuisioner untuk mengukur level kematangan dari prosedur pengamanan yang sudah dilakukan. Kriteria penilaiannya di sesuaikan dengan kriteria penilaian CMM yang terdiri dari level 0 hingga level 5. Selanjutnya menggunakan form audit checklist untuk mengukur kondisi keamanan dari infrastuktur jaringan berupa mikrotik dan komputer. Kriteria penilaiannya adalah dengan menggunakan skala *guttman*, jawaban memiliki kriteria tegas

yakni *yes* or *no*. selanjutnya akan dihitung persentase dari rata-rata setiap aspek yang dihitung berdasarkan hasil pengambilan data form audit dengan menggunakan rumus persentase

$$x = \frac{jk}{total} x\ 100\%$$

Dimana : x = Persentase pencapaian responden, jk = Jumlah keseluruhan skor yang di dapatkan dan total = Skor Maksimal.

B. Metode Pengumpulan Data

Dalam penelitian, teknik pengumpulan data merupakan faktor penting demi keberhasilan penelitian. Hal ini berkaitan dengan bagaimana cara mengumpulkan data, siapa sumbernya, dan apa alat yang digunakan sumber data adalah mengenai dari mana data diperoleh. Apakah data diperoleh dari sumber langsung (data primer) atau data diperoleh dari sumber tidak langsung (data sekunder).

Metode Pengumpulan Data merupakan teknik atau cara yang dilakukan untuk mengumpulkan data. Metode menunjuk suatu cara sehingga dapat diperlihatkan penggunaannya melalui angket, wawancara, pengamatan, tes, dokumentasi dan sebagainya. Sedangkan Instrumen Pengumpul Data merupakan alat yang digunakan untuk mengumpulkan data. Karena berupa alat, maka instrumen dapat berupa lembar cek list, kuesioner (angket terbuka atau tertutup), pedoman wawancara, kamera foto dan lainnya. Adapun dua teknik pengumpulan data yang digunakan adalah pengamatan dan dokumentasi screenshoot. Berikut penjelasan dibawah ini.

1. Observasi

   Metode observasi adalah melihat dan mendengarkan peristiwa atau tindakan yang dilakuakan oleh orang-orang yang diamati, kemudian merekam hasil pengamatannya dengan catatan atau alat bantu lainnya.

2. Kusesioner Responden

   Kuesioner merupakan metode pengumpulan data yang dilakukan dengan cara memberi beberapa pertanyaan atau pernyataan tertulis kepada responden untuk dijawab. Yang dimana jawaban tersebut digunakan untuk mengukur sikap terhadap perancangan sistem yang dibuat.

3. Dokumentasi

   Studi dokumen adalah metode pengumpulan data yang tidak ditujukan langsung kepada subjek penelitian. Studi dokumen adalah jenis pengumpulan data yang meneliti berbagai macam dokumen yang berguna untuk bahan analisis. Dokumen yang dapat digunakan dalam pengumpulan data dibedakan menjadi dua, yakni:

   a. Dokumen primer

      Dokumen primer yang penulis gunakan dalam penelitian ini yaitu Jurnal yang berhubungan dengan keamanan jaringan.

   b. Dokumen sekunder

      Dokumen sekunder yang penulis gunakan yaitu Buku pedoman jaringan komputer Telkom Indonesia.

C. Tinjauan Umum

Taman Pasuk Kameluh yang ada di bantaran Sungai Kahayan berdekatan dengan Tugu Soekarno, setiap hari selalu ramai dikunjungi warga yang ingin bersantai sambil menikmati suasana Sungai Kahayan. Taman Pasuk Kameluh, adalah salah satu tempat destinasi wisata yang ada di kota Palangka Raya. Tempat ini menjadi salah satu tempat iconik kota Palangka Raya. Taman Pasuk Kameluh diambil dari bahasa Dayak. Memiliki makna bakul gadis, yang artinya barang yang dimiliki seorang gadis. Kameloh lebih identik dekat dengan bakul perempuan cantik. Namun sebagian masyarakat juga mengartikan Pasuk Kameloh seperti kantong semar yang mengeluarkan panorama keindahan. Taman Pasuk Kameluh menyediakan lahan parkir dan juga toilet umum. Tersedia juga masjid bagi pengunjung yang ingin melaksanakan ibadah. Di taman ini memancar wifi dan terdapat kamera CCTV. Di bawah jembatan Kahayan terhampar kawasan kuliner khas Kalimantan.

Pada taman pasuk kameluh terdapat jaringan bebas yang disedaikan kolaborasi Pemerintah Kota dan Telkom Indonesia yang mana diperuntukan bagi pengunjung taman tersebut.

D. Analisis

1. Analisis keamanan jaringan yang sedang berjalan

   Sistem keamanan jaringan pada saat ini masih kurang efektif dan efisien dalam mensimulasikan tingkat keamanan pada jaringan internet. Dimana

keamanan jaringannya masih memiliki celah yang dapat disusupi pihak-pihak yang tidak bertanggung jawab.

Maka dari itu penulis mengangkat judul ini agar dilaksanakannya penelitian terhadap keamanan jaringan terbuka pada taman pasuk kameluh menggunakan *tool wireshark.*

2. Analsis sistem yang diusulkan

Analisis sistem yang diusulkan yaitu identifikasi celah keamanan jaringan pada website dengan tools packet sniffer untuk mengaudit keamanan jaringan dan memblokir lalu lintas jaringan yang dianggap sebagai ancaman dalam jaringan internet serta melakukan pengecekan terhadap kesalahan pada bagian media, wireless, dan media koneksinya.

3. Analisis Kebutuhan Analisis

Analisis kebutuhan analisis sangat diperlukan dalam mendukung analisis algoritma, apakah telah sesuai dengan kebutuhan atau belum. Karena kebutuhan analisis akan mendukung tercapainya tujuan.

a. Kebutuhan Perangkat Keras

Kebutuhan perangkat keras yang digunakan untuk menganalisis keamanan jaringan fasilitas sosial berikut dibawah ini.

1) Processor Intel Core i3 2.3GHz atau lebih
2) RAM minimal 2GB
3) Harddisk Minimal 8GB untuk instalasi software
4) Wifi Dongel Wireless
5) Windows 8.1 atau lebih

b. Kebutuhan Perangkat Lunak

Kebutuhan perangkat lunak yang digunakan untuk menganalisis keamanan jaringan fasilitas sosial berikut dibawah ini.

1) WireShark
2) NetCap
3) Google Chrome
4) Cisco Packet Tracker

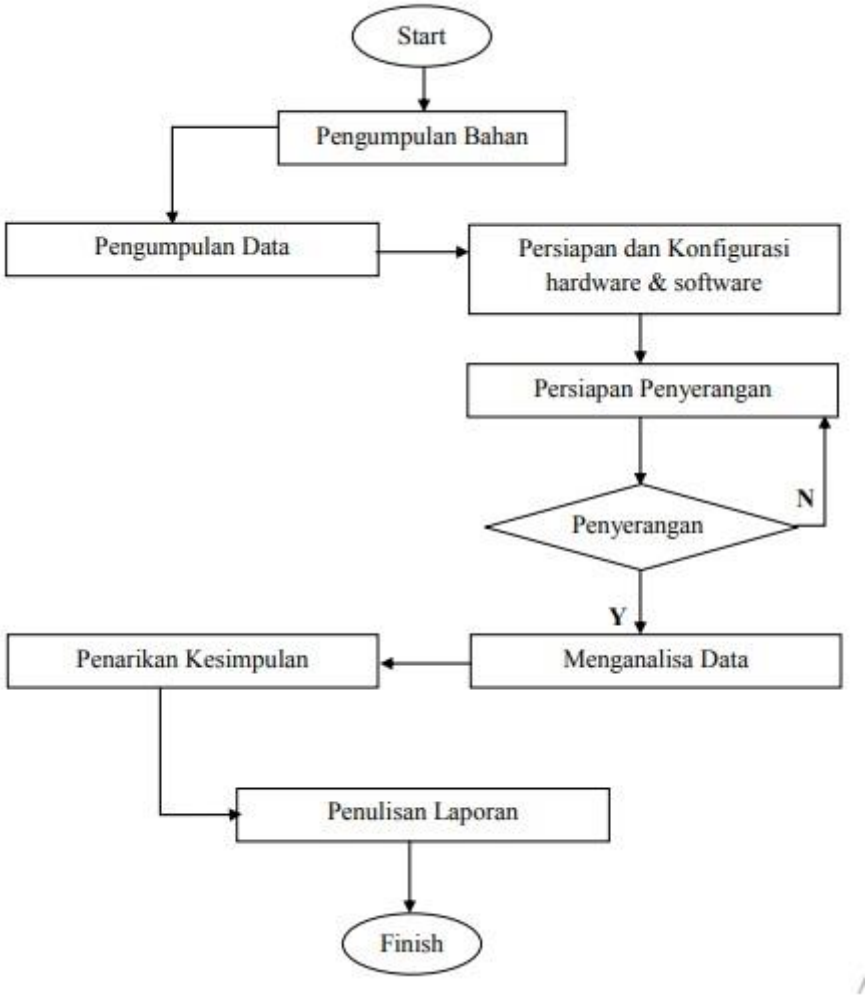
c. Kebutuhan Informasi

Kebutuhan informasi yang dibutuhkan penulis antara lain.

1) Literasi tentang Wireshark
2) Literasi tentang Jaringan Komputer

4. Kerangka Pemikiran dan flowchart

Dalam menjelaskan sebuah permasalahan kerangka pemikiran atau alur penelitian disajikan untuk mempermudah pemahaman dalam penelitian tersebut. Metode tersebut tersaji dalam diagram alir penelitian. Berikut dibawah ini.



Gambar 1. Flowchart Penelitian

5. Teknis Pengujian Keamanan

Pengujian keamanan bertujuan untuk memperoleh kesadaran akan permasalahan keamanan pada jaringan kabel dan nirkabel (wireless LAN).

a. Kuota penggunaan data tidak ditentukan dikarenakan bersifat bebas pakai oleh Kominfo Kota Palangka Raya menggunakan jaringan *Wifi.id* Telkom Indonesia (Penyedia layanan Internet).

b. Penyedia layanan internet *Wifi.id* tidak memberikan data pengguna, tetapi disini yang di analisis adalah pengunjung acak yang mengakses jaringan bebas pakai di sediakan oleh Kominfo Kota Palangka Raya.
c. Penulis mencoba mengidentifikasi keberadaan dan keamanan yang digunakan wifi target dengan menggunakan software Wireshark.
d. Setelah mengetahui keberadaan dan keamanan yang digunakan wifi target, penulis masuk untuk mendapatkan koneksi dengan wifi target.
e. Langkah pengujian keamanan, setelah mendapatkan koneksi dengan wifi target, penulis mencoba melakukan serangan Packet Sniffing terhadap wifi dan jaringan kabel dengan menggunakan software ettercap, serangan akan berhasil jika transfer data tidak dilindungi oleh keamanan seperti SSL, IPSec, WEP, WPA dan WPA2. Karena data yang didapat terenkripsi

BAB IV

IMPLEMENTASI DAN PEMBAHASAN

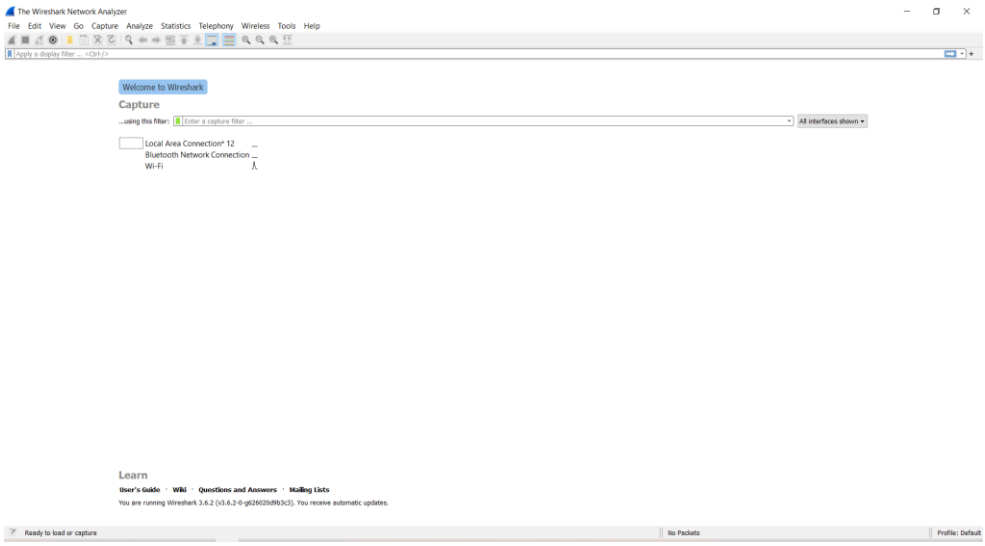
A. Hasil

1. Pengujian sistem keamanan jaringan *hotspot*

   Sistem keamanan jaringan *hotspot* yang sudah dikonfigurasi sebelumnya akan diuji dengan memantau *trafik ARP (Address Resolution Protocol)* pada jaringan dengan menggunakan aplikasi *wireshark*. Ukuran keberhasilan pengujian metode yang akan diterapkan yaitu dengan membandingkan jumlah *ARP (Address Resolution Protocol)* yang diterima sebelum dan setelah penerapan metode .

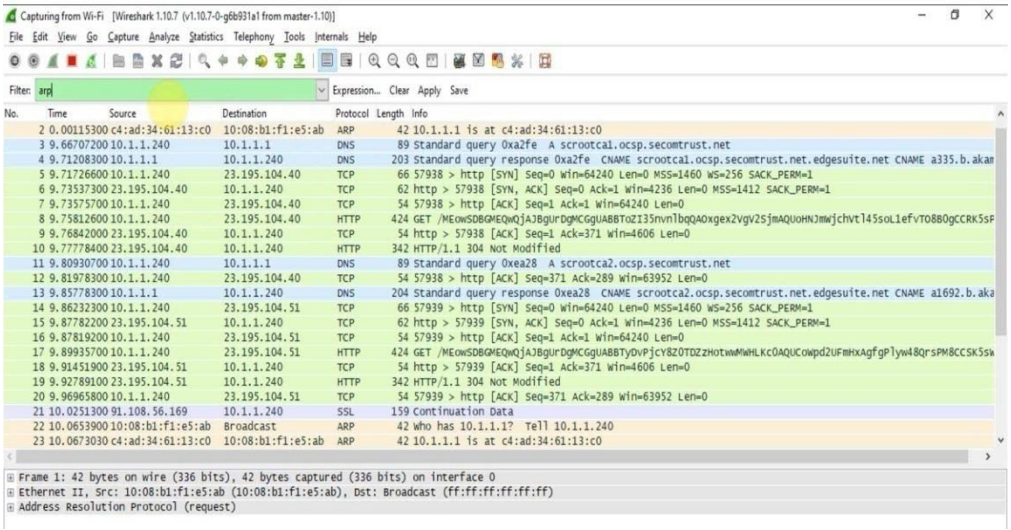
   1) Monitoring paket *ARP (Address Resolution Protocol)*

      Buka aplikasi *wireshark* kemudian pilih *wireless (wifi)* lalu klik *start*.



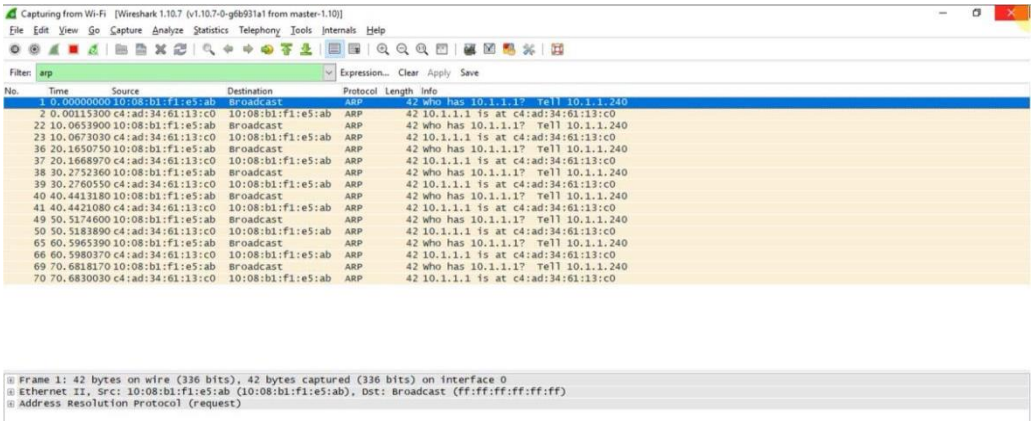
Gambar 2. Tampilan awal aplikasi *wireshark*

Selanjutnya akan muncul tampilan seluruh protokol yang ada pada jaringan *wifi* diantaranya *TCP,DNS,ARP*, dll. Untuk melihat seluruh Protokol *ARP* secara spesifik kita dapat mengetikkan *arp* pada *filter* kemudian *enter*.



Gambar 3. Tampilan semua protokol di aplikasi *wireshark*

Setelah itu akan muncul semua protokol *ARP* secara spesifik. Pada gambar berikut ini merupakan proses komunikasi yang stabil antara *client* dan *router* sebelum penyerangan *ARP Spoofing*.

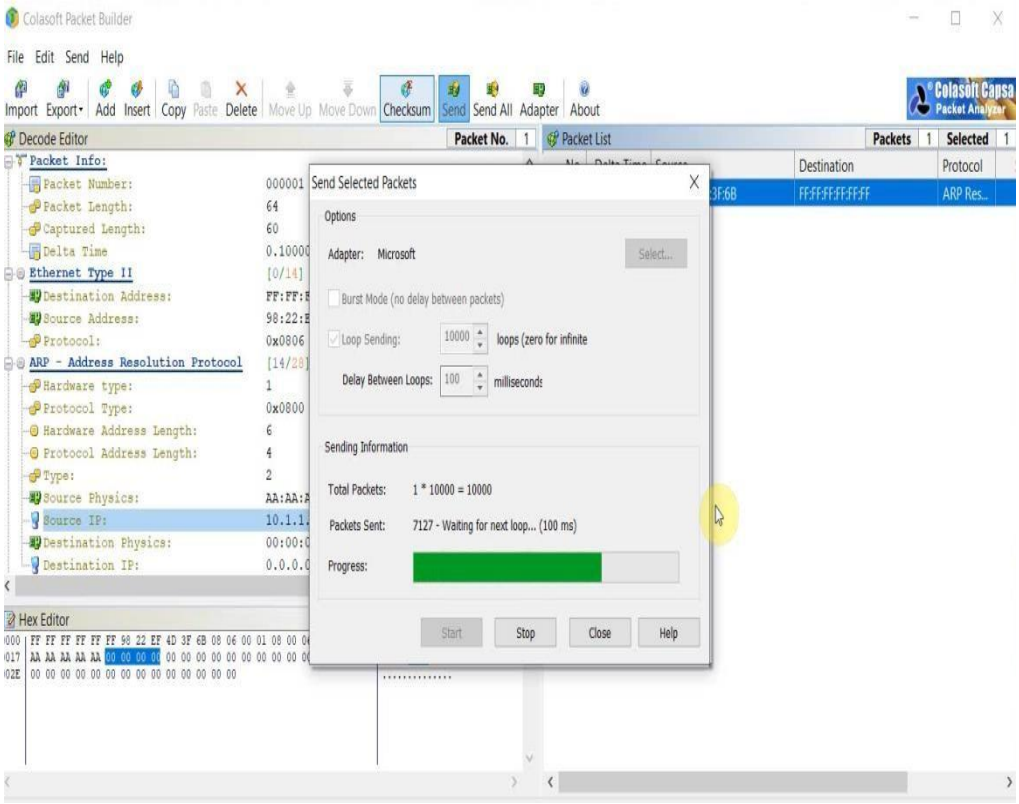


Gambar 4. Kondisi Koneksi stabil

2) Proses Spoofing

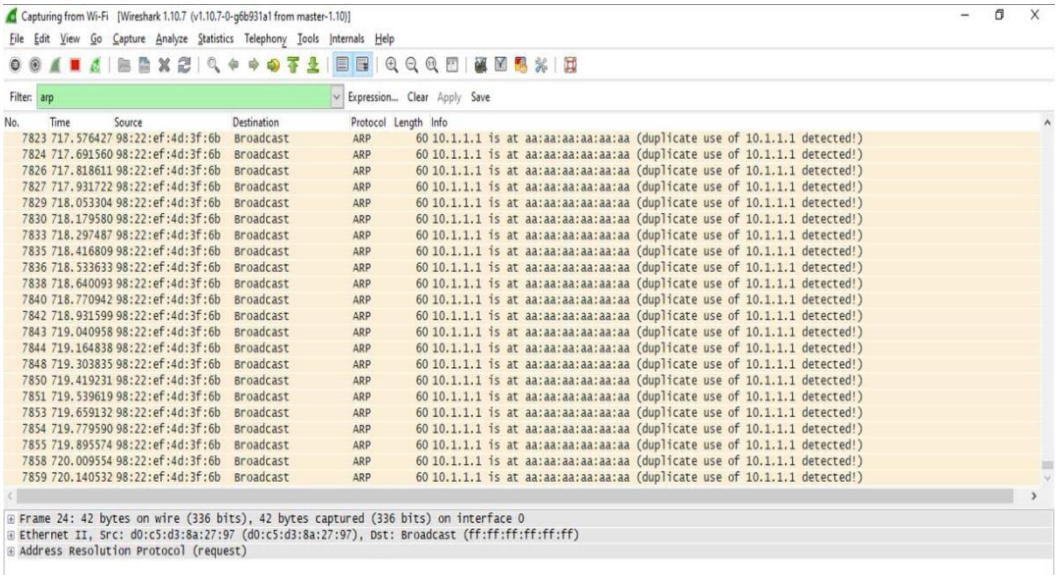
Pengiriman paket ARP paslu oleh spoofer yakni 10000 paket dalam 100 milisecond untuk merusak proses komnikasi secara broadcase antara pengguna jaringan hotspot lainyya dengan mikrotik. Ketika *Client* 1 mencari *macc address* mikrotik proses kominkasi dalam jaringan bisa digambarkan misalnya client 1 dengan IP 10.1.1.240 meminta mac address ke mikrotik dengan IP 10.1.1.1. Untuk pencarian *mac address* 10.1.1.1 *client* mengirim pesan secara *broadcase* ke semua perangkat dalam suatu jaringan mikrotik merupakan salah satunya. Siapa yang saat ini memaikai IP 10.1.1.1? hubungi saya di IP 10.1.1.240 kurang lebih seperti itu proses komunikasinya. Pada saat itu mikrotik akan secra otomatis mencatat *IP* dan *mac address* 10.1.1.240 di table *ARP (Address Resolution Protocol)* nya lalu selanjutnya mikrotik yang saat ini menggunakan IP tersebut akan membalas pesan dengan mengirim mac addressnya ke client 10.1.1.240 dan 10.1.1240 menerima mac addres dari 10.1.1.1 lalu menyimpannya di tabel *ARP (Address Resolution Protocol)*. Table *ARP (Address Resolution Protocol)* setiap perangkat akan melakukan *update* ketika masih menggunakan layanan dhcp dan itu akan menjadi celah spoofer untuk merusak komunikasi *ARP (Address Resolution Protocol)*. Celah *spoofer* untuk merusak komunikasi tersebut dengan mengirim langsung ke semua *client* paket palsu *macc address* yang sudah dimodifikasi menggunakan aplikasi *Colasoft*

Packet Builder 2.0. *spoofer* masuk ketika table *ARP (Address Resolution Protocol)* client masih belum lengkap saat melakukan update.



Gambar 5. Proses pemalsuan *mac address*

Berikut merupakan proses pemalsuan *mac address* yang dilakukan *spoofer*. Konfigurasi seperti yang telah lakukan di atas masih banyak diterapkan oleh penyedia layanan jaringan hotspot sampai saat ini. Oleh karena itu perlu pengamanan pada mikrotik agara ancaman terhadap *ARP (Address Resolution Protocol) Soofing* bisa teratasi.



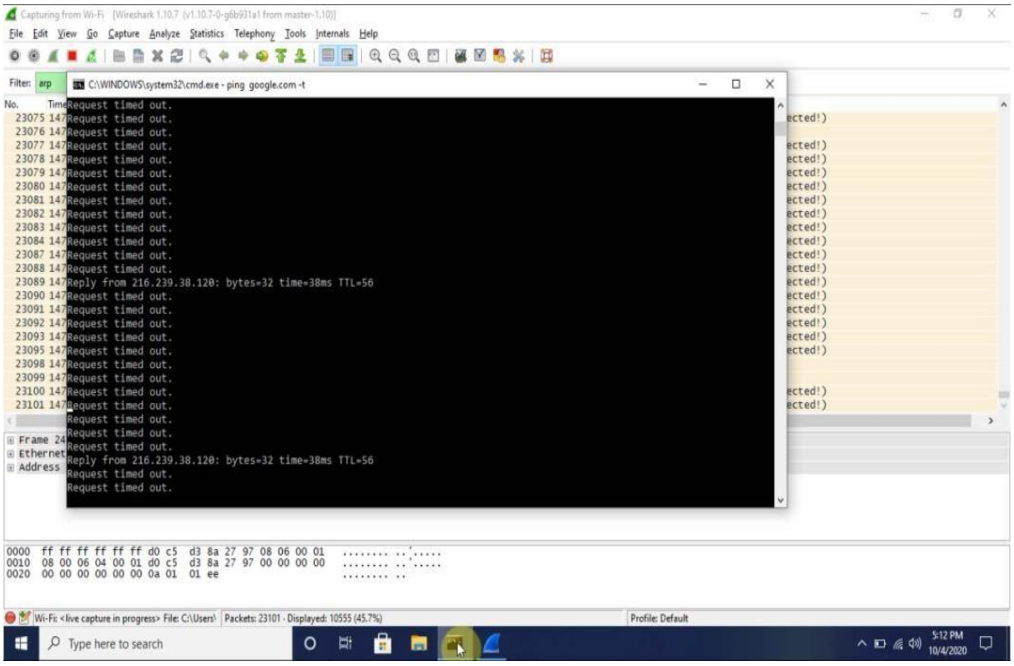
Gambar 6. Kondisi Koneksi pemalsuan *mac address*

3) Pengujian Koneksi Client

Penelitian ini dambil dari empat sampel laptop client yang sedang terkoneksi ke internet dan satu laptop spoofing yang sedang melakukan serangan pemalsuan mac addres terhadap empat laptop client. Berikut merupakan hasil uji koneksi dari proses serangan ARP Spoofing atau pemalusan Mac Address yang dilakukan Laptop Spoofer.

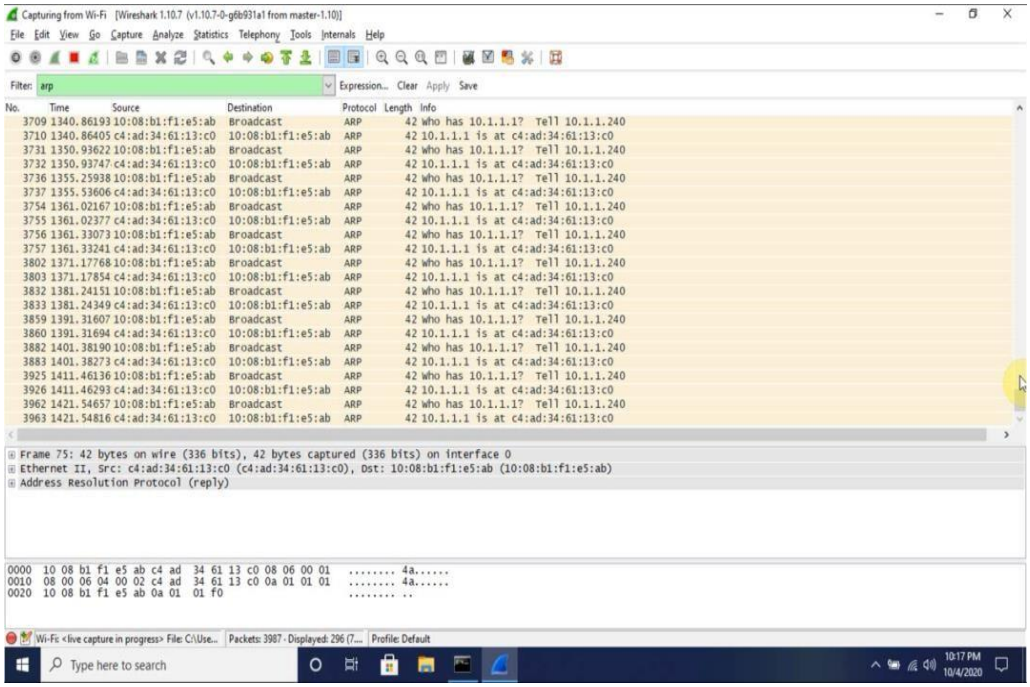
a) Laptop 1

Laptop pertama sebelum penerapan metode dapat dilihat jumlah *ARP (Address Resolution Protocol) Displayed* yang diterima sebanyak 10853 Paket *ARP (Address Resolution Protocol)* dan terlihat koneksi ke internet tersendat.



Gambar 7. Sebelum penerapan metode laptop 1

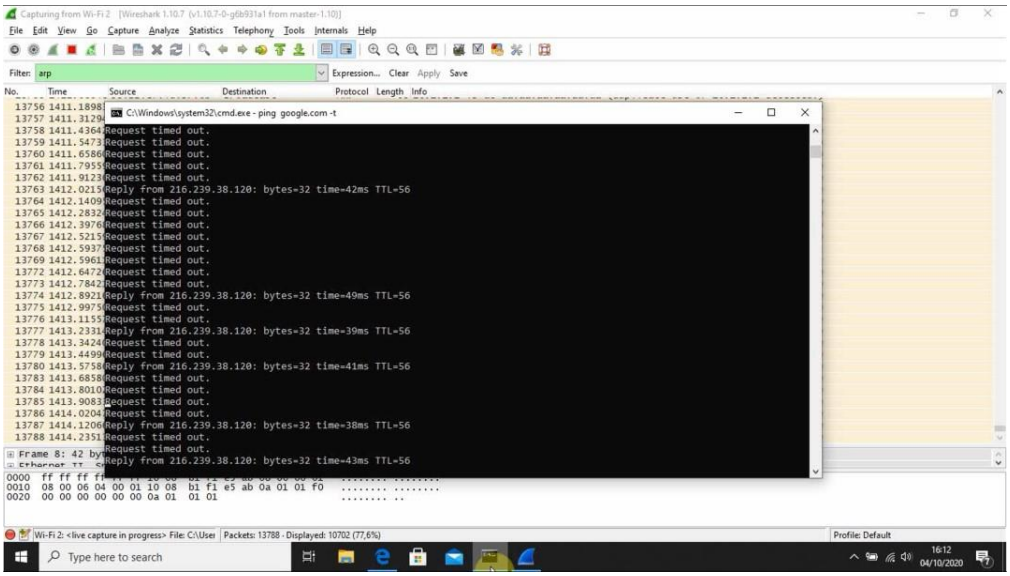
Setelah Penerapan metode jumlah *ARP (Address Resolution Protocol)* normal dari serangan sebanyak 296 Paket dan koneksi stabil.



Gambar 8. Jumlah *ARP* normal laptop 1

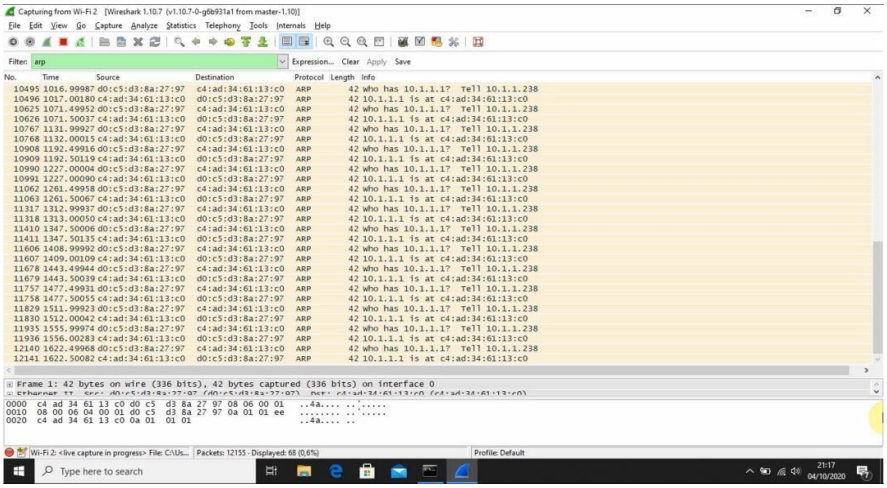
b) Laptop 2

Percobaan serangan laptop ketiga sebelum penerapan metode dapat dilihat jumlah ARP Displayed yang diterima sebanyak 10702 Paket ARP dan terlihat koneksi ke internet tersendat.



Gambar 9. Sebelum penerapan metode laptop 3

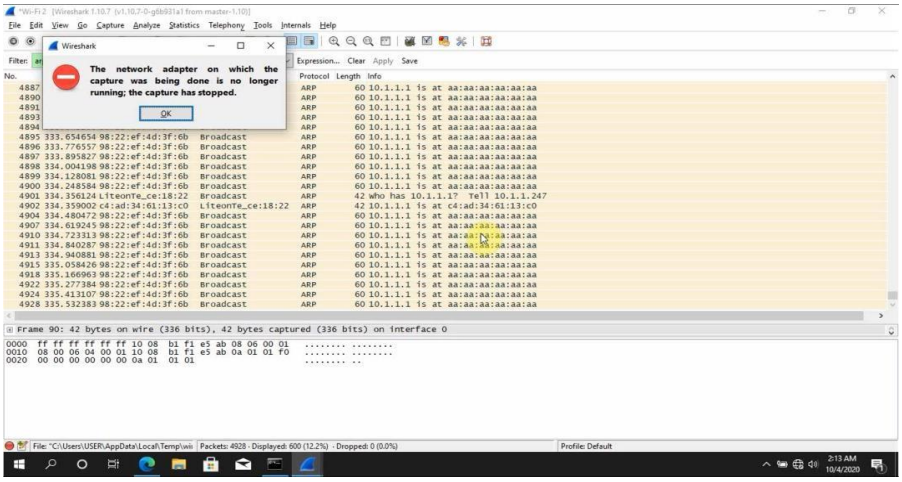
Setelah Penerapan metode jumlah ARP normal dari serangan sebanyak 68 Paket dan koneksi stabil



Gambar 10. Jumlah ARP normal laptop 3

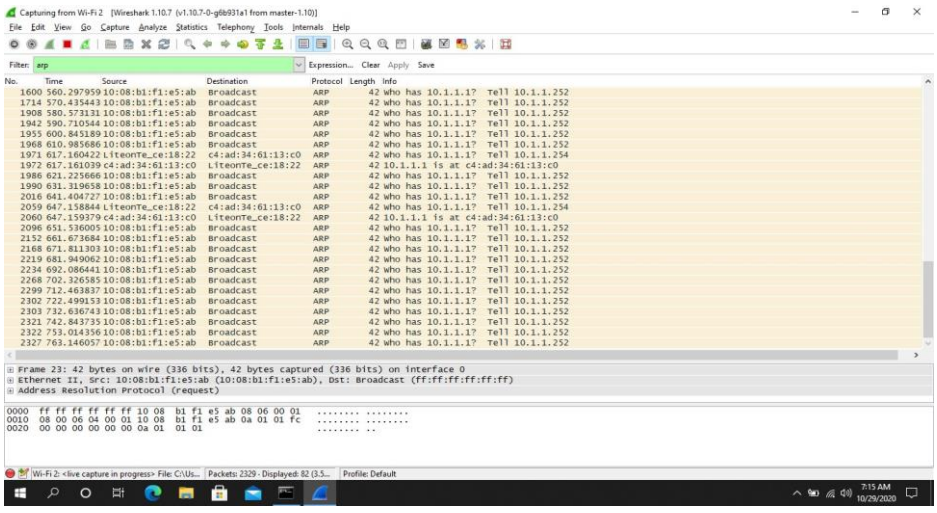
c) Laptop 3

Percobaan serangan laptop keempat sebelum penerapan metode dapat dilihat jumlah *ARP (Address Resolution Protocol) Displayed* yang diterima sebanyak 600 Paket *ARP (Address Resolution Protocol)* dan terlihat koneksi ke internet terputus.



Gambar 11. Sebelum penerapan metode laptop 4

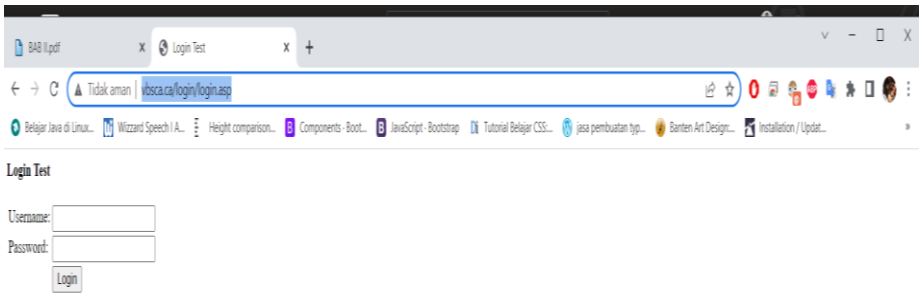
Setelah Penerapan metode jumlah *ARP (Address Resolution Protocol)* normal dari serangan sebanyak 82 Paket dan koneksi stabil



Gambar 12. Jumlah *ARP* normal laptop 4

4) Pengecekan Website

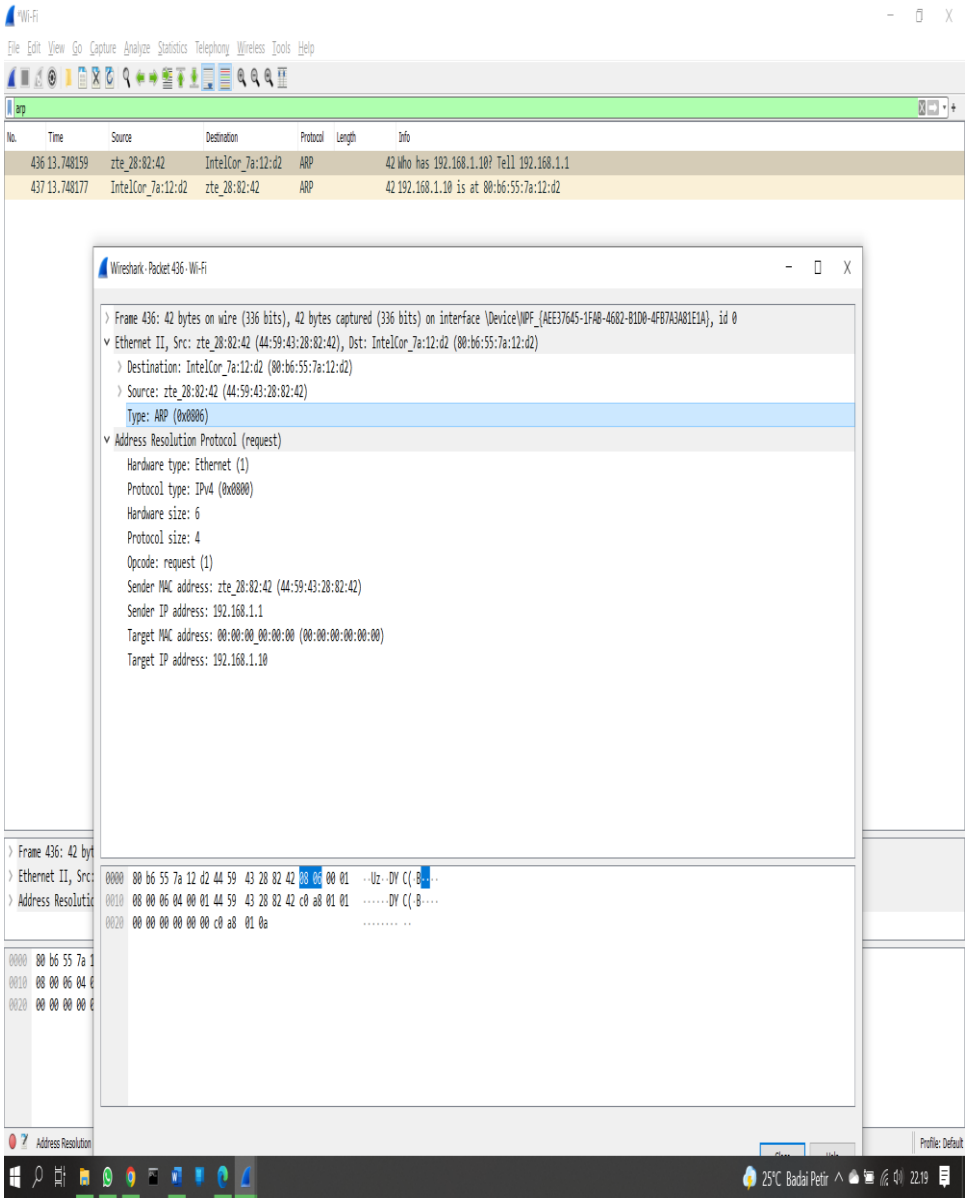
Pada tahap selanjutnya penulis menguji salah satu link yang mudah di sniifing menggunakan ARP pada wireshark dengan link : http://www.vbsca.ca/login/login.asp.



Gambar 13. Proses Pengecekan Form Login

Login Test

Sorry, but the username that you entered does not exist.



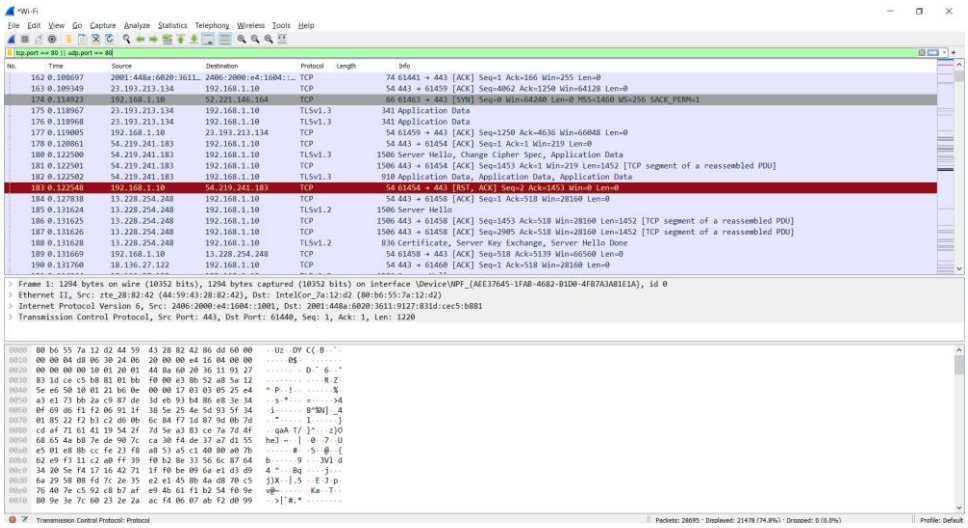
Gambar 14. Proses Pengecekan Pada Wireshark

B. Pembahasan

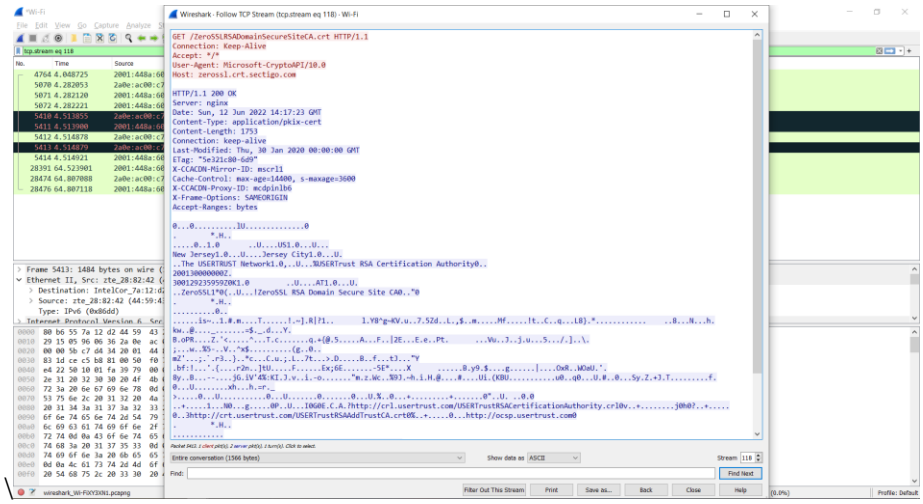
1. Pengujian Kelayakan Prosedur (QoS)

   a. Yahoo

   Pada tahap ini di ujikan mengirim sebuah filed username pada inputan login, dan hasilnnya tidak ada data yang dikirim memnandakan bahwa protokol yang digunakan oleh situs yahoo.com aman untuk di isi data username dan password, dapat dilihat pada gambar dibawah ini :



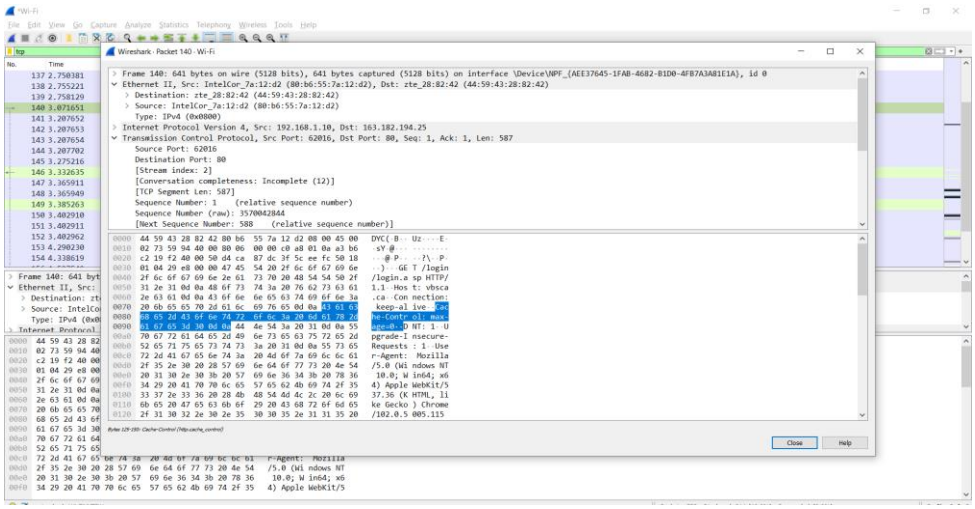
Gambar 15. Proses Pengecekan Yahoo.com



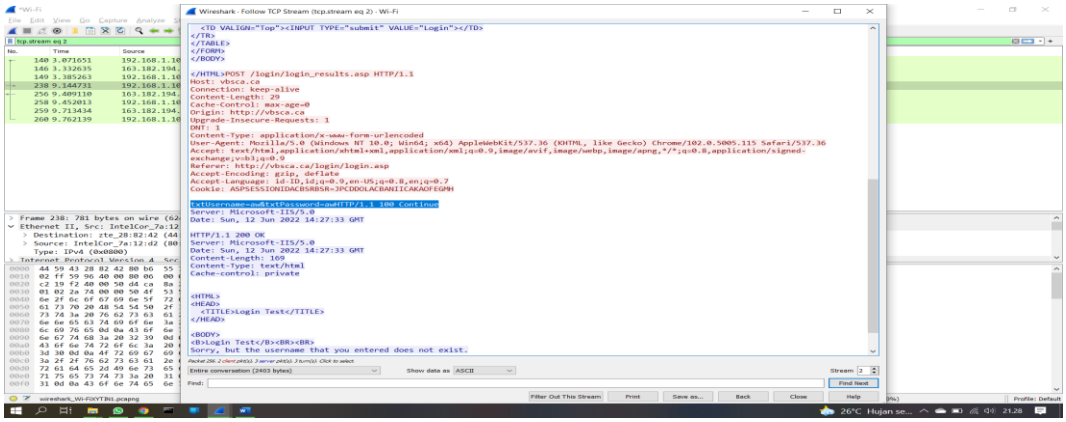
Gambar 16. Proses Pengecekan Following Yahoo.com

b. Login TestPage.com

Pada tahap ini di ujikan mengirim sebuah filed username pada inputan login, dan sniifing menggunakan ARP pada wireshark hasilnnya menunjukkan bahwa data yang dikirim direkam dan ada data yang dikirim memnandakan bahwa protokol yang digunakan oleh situs Login test tidak aman untuk di isi data username dan password, dapat dilihat pada gambar dibawah ini :



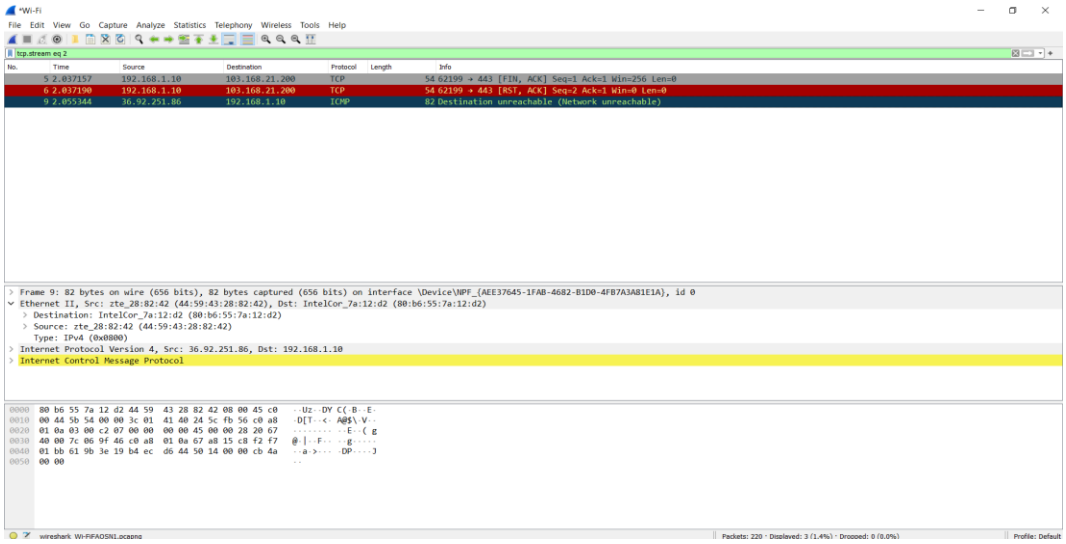
Gambar 17. Proses Pengecekan Yahoo.com



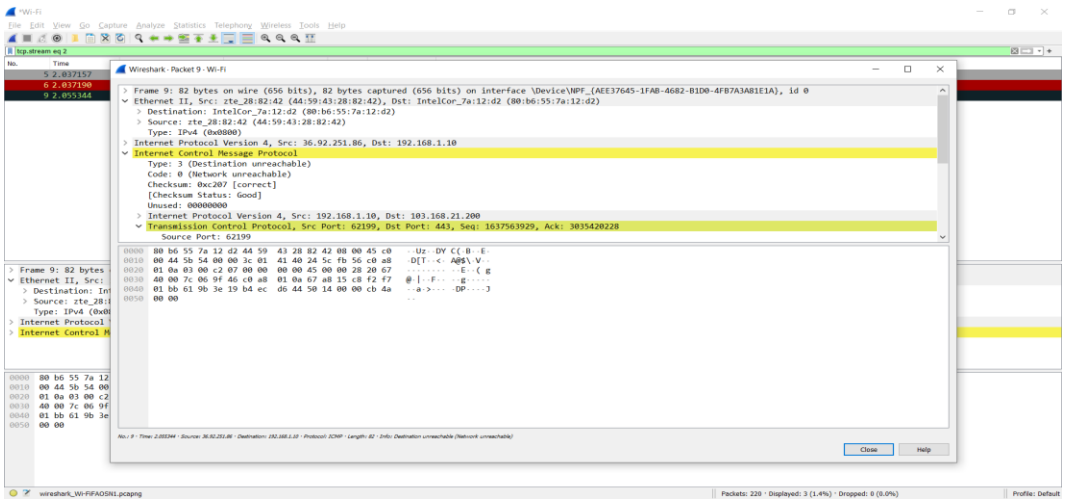
Gambar 18. Proses Pengecekan Data terbaca oleh Wireshark

c. Smart Stmik Palangkaraya

Pada tahap ini di ujikan mengirim sebuah filed username pada inputan login, dan hasilnnya tidak ada data yang dikirim memnandakan bahwa protokol yang digunakan oleh situs Smart Stmik Palangkaraya aman untuk di isi data username dan password, dapat dilihat pada gambar dibawah ini:



Gambar 19. Proses Pengecekan Smart.Stmik.plk



Gambar 20. Proses Pengecekan tidak ada data yang diterima

2. Pembahasan Hasil Penelitian Jaringan WEP

Dari hasil penelitian maka penulis memberikan beberapa interpretasi hasil dari penelitian yang dilakukan melalui pengujian langsung. Untuk sistem keamanan jaringan menggunakan WEP memiliki teknik enkripsi yang sangat rentan, dikarenakan pada pengujian yang dilakukan di Taman Pasuk Kameloh Palangkaraya yang menggunakan sistem keamanan jaringan WEP, masih dapat diketahui password melalui proses enkripsi. Sistem keamanan jaringan WEP ini menggunakan kunci yang bersifat statis dan sangat tidak cocok untuk keamanan jaringan bersifat umum atau khusus. Sistem ini sebaiknya digunakan untuk pelatihan bagi hotspot pemula. Sedangkan untuk sistem keamanan WPA memiliki teknik enkripsi yang baik, sehingga dalam proses pengujian tidak didapatkan hasil. Keamanan jaringan WPA ini baiknya digunakan untuk jaringan hotspot yang bersifat umum atau dalam ruangan dan sinyal tidak terlampau ke luar ruangan. Sistem keamanan RADIUS sistem ini sangat cocok digunakan untuk jaringan hotspot di sekolah atau di universitas, dikarenakan sistem ini memiliki database user yang terdaftar berupa username dan password, Sehingga user yang tidak terdaftar di database tidak dapat melakukan akses pada jaringan. Sistem keamanan ini akan mempermudah bagi administrator dalam memantau client dan menganalisa setiap gangguan yang muncul.

3. Pembahasan Hasil DHCP Dan Wireshark

ARP Spoofing melakukan serangan pemalsuan mac addrees dengan memanfaatkan layer 2 di router mikrotik yang masih terbuka pada konfigurasi standart yang umum dipakai saat ini. Untuk melakukan

pencegahan pemalsuan mac address pada jaringan hotspot dapat dilakukan pembatasan atau isolasi komunikasi antar client dan mikrotik. Dengan mengaktifkan AP Isolation dan ARP Static pada konfigurasi mikrotik dapat mencegah ARP Spoofing. AP Isolation merupakan teknik atau metode pengisolasian antar client yang terkoneksi pada wireless accsess point. Penerapa ARP Static pada jaringan dilakukan agar mirkrotik tidak melakukan pencarian ARP lagi pada layanan Dhcp Server dikarenakan mikrotik sudah mencatat secara Static di ARP table. ARP table pada mikrotik rentan terhadap serangan ketika masih menggunakan DHCP karena ketika masih DHCP pada layananya ARP table akan terus melakukan update pencarian ARP baru sehingga ARP Spoofing bisa masuk kedalam celah tersebut untuk mengacaukan komunikasi antar client dan router. Oleh karena itu harus mengatur secara static pada layanan DHCP agar ARP table tidak melakukan update saat sedang koneksi ke internet. Dengan ini komunikasi antar client akan dibatasi oleh mikrotik agar Spoofer tidak bisa lagi melakukan serangan sehingga koneksi pengguna pada jaringan hotspot bisa terkendali.

4. Pembahasan Hasil Response Pengguna

Berikut ini adalah pembahasan dari penelitian dan juga pembahasan mengenai kuesioner dengan perhitungan skala *likert* yang dibuat penulis, Dengan menggunakan Skala *Likert*, variabel yang akan diukur dijabarkan menjadi dimensi, lalu dijabarkan menjadi subvariabel dan subvariabel dijabarkan lagi menjadi indikator yang dapat diukur. Pada akhirnya, indikator-indikator yang terukur dapat menjadi titik tolak untuk membuat

item instrument berupa pernyataan atau pertanyaan yang perlu dijawab oleh responden. Berdasarkan jawaban dari responden terhadap kepuasan pengguna dapat diukur dengan menggunakan ketentuan sebagai berikut:

Tabel 2. Ukuran Ketentuan Kriteria Responden

No.	Pertanyaan
1.	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan
2.	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan
3.	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik
4.	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi
5.	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.
6.	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif

Keterangan bobot penilaian :

Keterangan	Nilai
Sangat Setuju	5
Setuju	4
Netral	3
Tidak Setuju	2
Sangat tidak setuju	1

Selanjutnya hasil jawaban tersebut diolah dan dihitung dengan kriteria total dari 15 responden yang telah ditetapkan pada tabel 3 pernyataan kuesioner responden dibawah ini.

Tabel 3. Pertanyaan Kuesioner Responden

No	Point Pertanyaan	Responden															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Total
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	5	4	5	5	5	5	4	5	5	5	5	4	5	5	4	71
2.	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan	5	4	5	4	5	5	4	4	5	5	5	4	5	5	5	70
3.	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik	5	5	5	5	5	5	4	5	5	4	5	4	4	4	5	70
4.	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	74
5.	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	74
6.	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif	5	5	4	4	5	4	5	5	5	4	4	4	4	5	5	68
Skor Akhir Pengumpulan Data																	427

Jumlah skor tertinggi tiap pernyataan = Skor tertinggi tiap pernyataan x jumlah responden = 5 x 15 = 75 > (SS)

Jumlah skor terendah tiap pernyataan = Skor terendah tiap pernyataan x jumlah responden = 1 x 15 =15 > (STS)

Sehingga kriteria interpretasi skor untuk setiap item pernyataan adalah sebagai berikut :

Angka 0 - 15 = Sangat Tidak Setuju (STS)

Angka 16 – 30 = Tidak Setuju (TS)

Angka 31 – 45 = Netral (N)

Angka 46 – 60 = Setuju (S)

Angka 61 – 75 = Sangat Setuju (SS)

Berdasarkan data yang diperoleh dari 15 responden maka dapat diketahui bahwa :

1. Pernyataan ke-1 dengan jumlah skor 71 terletak pada daerah “Sangat Setuju”
2. Pernyataan ke-2 dengan jumlah skor 70 terletak pada daerah “Sangat Setuju”
3. Pernyataan ke-3 dengan jumlah skor 70 terletak pada daerah “Sangat Setuju”
4. Pernyataan ke-4 dengan jumlah skor 74 terletak pada daerah “Sangat Setuju”
5. Pernyataan ke-5 dengan jumlah skor 74 terletak pada daerah “Sangat Setuju”
6. Pernyataan ke-6 dengan jumlah skor 68 terletak pada daerah “Sangat Setuju”

Untuk hasil skor secara keseluruhan adalah sebagai berikut :

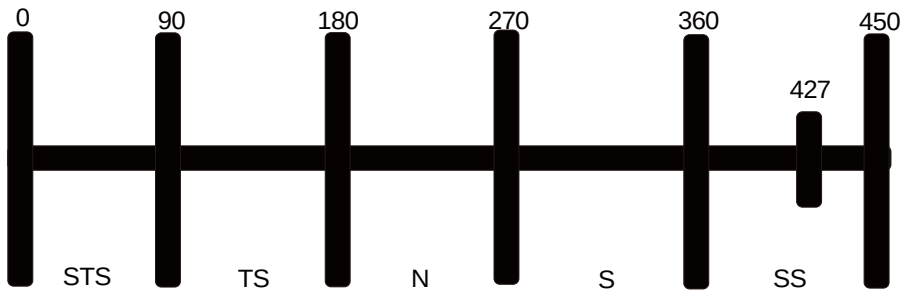
Jumlah skor tertinggi = skor tertinggi tiap item x jumlah responden x jumlah pernyataan = 5 x 15 x 6 = 450

Jumlah skor terendah = skor terendah tiap item x jumlah responden x jumlah pernyataan = 1 x 15 x 6 = 90

Sehingga kriteria interpretasi skor secara keseluruhan adalah sebagai
berikut :

0 – 90 = Sangat Tidak Setuju (STS)
91 – 180 = Tidak Setuju (TS)
181 – 270 = Netral (N)
271 – 360 = Setuju (S)
361 – 450 = Sangat Setuju (SS)

Dari kriteria tersebut maka dapat diketahui bahwah total skor keseluruhan yaitu 450 berada pada daerah sangat setuju. Adapun total skor keseluruhan dapat dilihat seperti dibawah ini:



Gambar 21. Pengukuran Skala *Likert* Responden

Dari skala di atas dapat diketahui bahwa angka 427 berada di daerah sangat setuju yang berarti secara keseluruhan rata-rata responden sangat setuju terhadap poin-poin pernyataan yang dimaksud

pada tabel 16. Adapun untuk mengetahui persentase kelompok responden untuk setiap item pernyataan adalah:

Persentase Kelompok Responden = (Jumlah Skor Tiap Pernyataan/Jumlah Skor tertinggi Tiap Pernyataan) x 100% Dengan kriteria interpretasi persentase kelompok responden adalah sebagai berikut:

Angka 0% - 20% = Sangat Tidak Baik (STB)

Angka 21% - 40% = Kurang Baik (KB)

Angka 41% - 60% = Cukup Baik (CB)

Angka 61% - 80% = Baik (B)

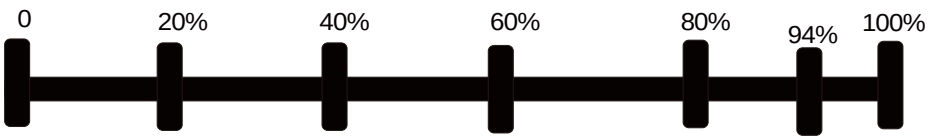
Angka 81% - 100% = Sangat Baik (SB)

Maka berdasarkan rumus perhitungan persentase kelompok responden tiap item pernyataan dapat diketahui bahwa:

1. Pernyataan ke-1, dengan jumlah skor 71/ 75 x 100 % = 94 % tergolong Sangat Baik (SB).
2. Pernyataan ke-2, dengan jumlah skor 70 / 75 x 100 % = 93 % tergolong Sangat Baik (SB).
3. Pernyataan ke-3, dengan jumlah skor 74 / 75 x 100 % =98% tergolong Sangat Baik (SB).
4. Pernyataan ke-4, dengan jumlah skor 74 / 75 x 100 % = 98 % tergolong Sangat Baik (SB)
5. Pernyataan ke-5, dengan jumlah skor 74/ 75 x 100 % = 98 % tergolong Sangat Baik (SB).

6. Pernyataan ke-6, dengan jumlah skor 68 / 75 x 100 % = 90 % tergolong Sangat Baik (SB).

Adapun untuk persentase kelompok responden secara keseluruhan: Total Skor Keseluruhan / Jumlah Skor Tertinggi Keseluruhan x 100 % = 427 / (75x6) x 100% = 94 % Maka persentase kelompok responden secara keseluruhan adalah 94% yang berarti tergolong sangat setuju. Adapun persentase kelompok responden untuk secara keseluruhan dapat dilihat seperti:



Dari skala di atas dapat diketahui bahwa hasil dari perhitungan kuesioner yang dinilai dari 15 responden dan 6 pernyataan maka diperoleh hasil interpretasi sebesar 94 % atau rata-rata responden memberikan hasil penilaian yang Sangat Baik terhadap sistem yang dikembangkan penulis.

BAB V

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan pemaparan dari bab - bab sebelumnya, maka penulis dapat menarik kesimpulan sebagai berikut:

1. ARP Spoofing melakukan serangan pemalsuan mac addrees dengan memanfaatkan layer 2 di router mikrotik yang masih terbuka pada konfigurasi standart yang umum dipakai saat ini.
2. Untuk melakukan pencegahan pemalsuan mac address pada jaringan hotspot dapat dilakukan pembatasan atau isolasi komunikasi antar client dan mikrotik. Dengan mengaktifkan AP Isolation dan ARP Static pada konfigurasi mikrotik dapat mencegah ARP Spoofing. AP Isolation merupakan teknik atau metode pengisolasian antar client yang terkoneksi pada wireless accsess point. Penerapa ARP Static pada jaringan dilakukan agar mirkrotik tidak melakukan pencarian ARP lagi pada layanan Dhcp Server dikarenakan mikrotik sudah mencatat secara Static di ARP table.
3. ARP table pada mikrotik rentan terhadap serangan ketika masih menggunakan DHCP karena ketika masih DHCP pada layananya ARP table akan terus melakukan update pencarian ARP baru sehingga ARP Spoofing bisa masuk kedalam celah tersebut untuk mengacaukan

komunikasi antar client dan router. Oleh karena itu harus mengatur secara static pada layanan DHCP agar ARP table tidak melakukan update saat sedang koneksi ke internet. Dengan ini komunikasi antar client akan dibatasi oleh mikrotik agar Spoofer tidak bisa lagi melakukan serangan sehingga koneksi pengguna pada jaringan hotspot bisa terkendali.

B. Saran

Adapun saran dan harapan yang diberikan penulis untuk penelitian selanjutnya adalah sebagai berikut :

1. Penelitian selanjutnya dapat menganalisis cara kerja ARP Spoofing dalam melakukan serangan pada layer 2 TCP/IP.
2. Penelitian selanjutnya dapat mencoba teknik serangan jaringan hotspot lainnya seperti ARP Poisoning atau sniffing dalam melakukakn penyadapan data melalui layer 2 pada protokol TCP/IP serta pengamanannya.

DAFTAR PUSTAKA

Agung Nugroho (2012).“Analisa Keamanan Jaringan Wireless Local Area Network Dengan Access Point Tp-Link Wa500g”. Skripsi Program Studi Teknik Informatika Fakultas Komunikasi Dan Informatika Universitas Muhammadiyah Surakarta

Arianto, Sam. 2008. Pengertian Fasilitas Belajar dan Jenisnya. Tersedia : http://sobatbaru.blogspot.com/2014/10/pengertian.fasilitas.belajar.html

Ayu Syifa Destiani (2015).“Analisis Protokol Keamanan Situ Unpas Dengan Menggunakan Sslstrip Dan Wireshark”. Skripsi Program Studi Teknik Informatika Fakultas Teknik Universitas Pasundan Bandung

Bayu Arie Nugroho (2012).“Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) Terhadap Serangan Packet Sniffing”. Skripsi Skripsi Program Studi Informatika Fakultas Komunikasi Dan Informatika Universitas Muhammadiyah Surakarta

Ferry, Astika & Iwan, Syarif Penerapan Proxy Server Dengan Menggunakan Squid. (online), (http://lecturer.eepis-its.edu/ diakses pada tanggal 5 Juni 2022)

Gilang Kumala Dewi (2016). “Analisa Keamanan Jaringan Wireless Di Sekolah Menengah Al Firdaus”. Skripsi Program Studi Informatika Fakultas Komunikasi Dan Informatika Universitas Muhammadiyah Surakarta

Kadir. Abdul. (2003). Pengenalan Sistem Informasi. Yogyakarta: Andi Offset.
Harahap, Sofyan Syafri. 2015. Analisis Kritis atas Laporan Keuangan. Edisi 1-10. Jakarta: Rajawali Pers.

Kustanto dan Daniel T saputro, 2015. Belajar Jaringan Komputer Berbasis Mikrotik OS. Yogyakarta: Gava Media.

M. R. Kurniawan (2018). “Analisis Sistem Keamanan Wireless Local Area Network (Wlan) Pada Proses Tethering”. Jurnal Jurusan Teknik Elektro Universitas Riau

Muslihudin, Muhammad, Oktafianto.2016. Analisis dan Perancangan Sistem Informasi Menggunakan Model Terstruktur dan UML. ANDI OFFSET. Yogyakarta.

Sam, Arianto. 2008. Pengertian Fasilitas Belajar dan Jenisnya. Tersedia : http://sobatbaru.blogspot.com/2014/10/p
engertian.fasilitas.belajar.htm. Diperoleh 25 November 2014.

Singh, K. U. (2014). LSB Audio Steganograpy Approach. ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014, ISSN 2250-2459.

Sofana, Iwan. 2013. Membangun Jaringan Komputer : Mudah membuat Jaringan Komputer (Wire & Wireless) untuk pengguna Windows dan Linux. Bandung: Informatika.

Yuni Fitriani. 2020. “Analisis Pemanfaatan Teknologi Informasi Dalam Pembelajaran Jarak Jauh Di Tengah Pandemi Virus Corona Covid-19”.

LAMPIRAN

Lampiran 1. Surat Tugas

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp. 0536-3225515 Fax. 0536-3225515 Palangkaraya
email : humas@stmikplk.ac.id – website : www. stmikplk.ac.id

SURAT TUGAS
No.307/STMIK-C.1/AK/II/2021

Ketua Program Studi Sistem Informasi Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan nama-nama tersebut di bawah ini :

1. Nama : Sam'ani, ST., M.Kom.
   NIK : 197703252005105
   Sebagai Pembimbing I dalam **Materi Penelitian dan Program**

2. Nama : Hafiz Riyadli, M.Kom.
   NIK : 198604042010103
   Sebagai Pembimbing II dalam **Format Penulisan**

Untuk membimbing Tugas Akhir Mahasiswa :

Nama	:	Liantoni
NIM	:	C1757201023
Judul Tugas Akhir	:	Analisis Keamanan Jaringan Publik Pada Fasilitas Sosial Di Kota Palangka Raya Menggunakan Wireshark
Berlaku s/d	:	24 Maret 2022

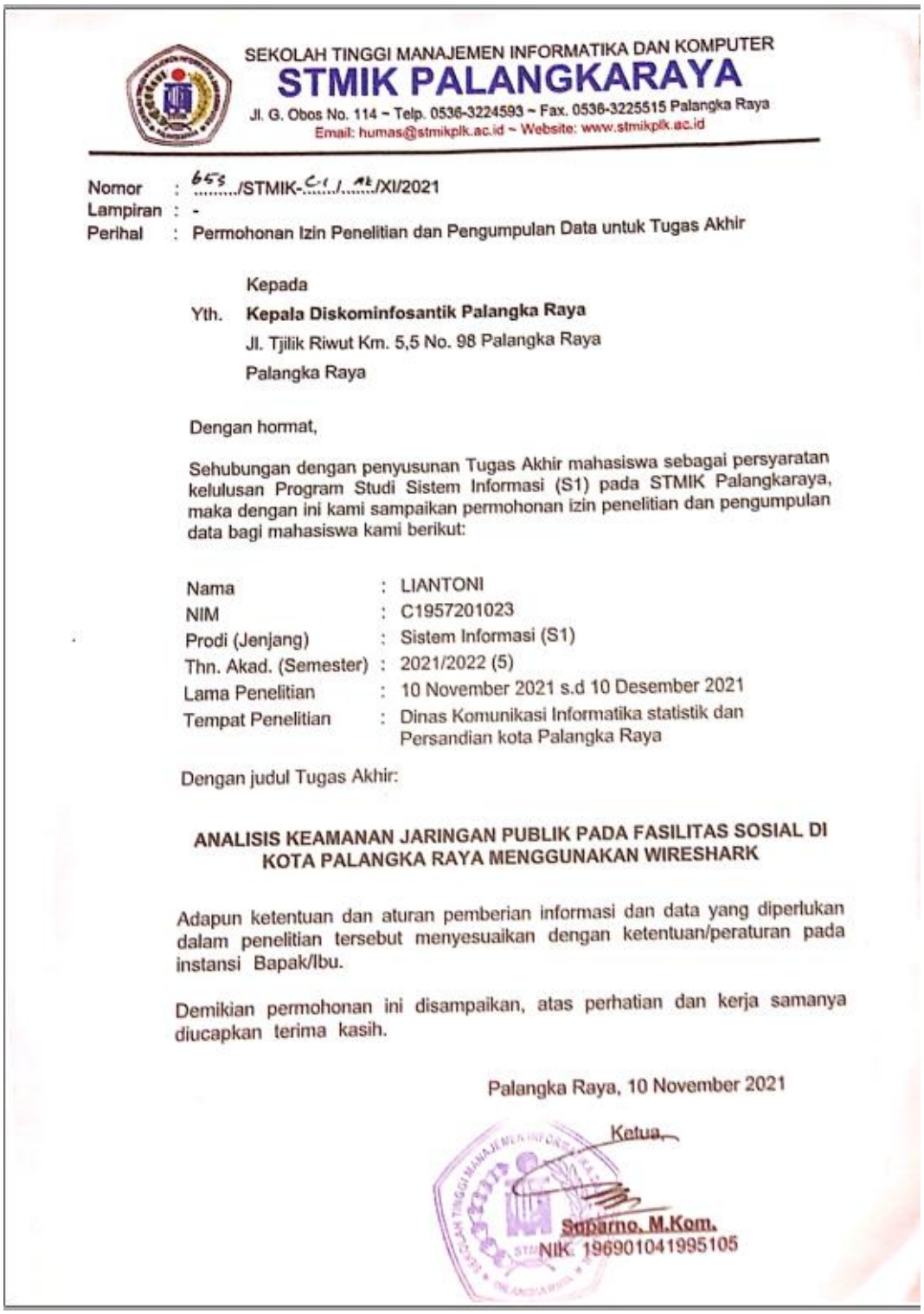
Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 24 Maret 2021
Ketua Program Studi
Sistem Informasi

Nor Hayati, M.Pd.
NIK. 198805222011004

Tembusan :
1. Ketua STMIK Palangkaraya
2. Kepala Unit Penjaminan Mutu Internal (UPMI)
3. Dosen Pembimbing yang bersangkutan
4. Arsip Program studi Sistem Informasi

Lampiran 2. Surat Permohonan Izin Penelitian



SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
STMIK PALANGKARAYA
Jl. G. Obos No. 114 ~ Telp. 0536-3224593 ~ Fax. 0536-3225515 Palangka Raya
Email: humas@stmikplk.ac.id ~ Website: www.stmikplk.ac.id

Nomor : 655/STMIK-C.1/PL/XI/2021
Lampiran : -
Perihal : Permohonan Izin Penelitian dan Pengumpulan Data untuk Tugas Akhir

Kepada
Yth. **Kepala Diskominfosantik Palangka Raya**
Jl. Tjilik Riwut Km. 5,5 No. 98 Palangka Raya
Palangka Raya

Dengan hormat,

Sehubungan dengan penyusunan Tugas Akhir mahasiswa sebagai persyaratan kelulusan Program Studi Sistem Informasi (S1) pada STMIK Palangkaraya, maka dengan ini kami sampaikan permohonan izin penelitian dan pengumpulan data bagi mahasiswa kami berikut:

Nama	:	LIANTONI
NIM	:	C1957201023
Prodi (Jenjang)	:	Sistem Informasi (S1)
Thn. Akad. (Semester)	:	2021/2022 (5)
Lama Penelitian	:	10 November 2021 s.d 10 Desember 2021
Tempat Penelitian	:	Dinas Komunikasi Informatika statistik dan Persandian kota Palangka Raya

Dengan judul Tugas Akhir:

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Adapun ketentuan dan aturan pemberian informasi dan data yang diperlukan dalam penelitian tersebut menyesuaikan dengan ketentuan/peraturan pada instansi Bapak/Ibu.

Demikian permohonan ini disampaikan, atas perhatian dan kerja samanya diucapkan terima kasih.

Palangka Raya, 10 November 2021

Ketua,

Suparno, M.Kom.
NIK. 196901041995105

Lampiran 3. Balasan Surat Izin Penelitian

PEMERINTAH KOTA PALANGKA RAYA
DINAS KOMUNIKASI, INFORMATIKA
STATISTIK DAN PERSANDIAN
Jl. Tjilik Riwut Km.5,5 No. 98 Palangka Raya
Website : www.palangkaraya.go.id

Palangka Raya, 29 November 2021

Nomor : 440/DKISP/XI/2021
Lampiran : -
Perihal : Pemberitahuan

Kepada,
Yth. Kepala STMIK Palangka Raya
Di-
Kota Palangka Raya

Sehubungan dengan pemintaan untuk izin penelitian mahasiswa atas nama :

Nama : LIANTONI

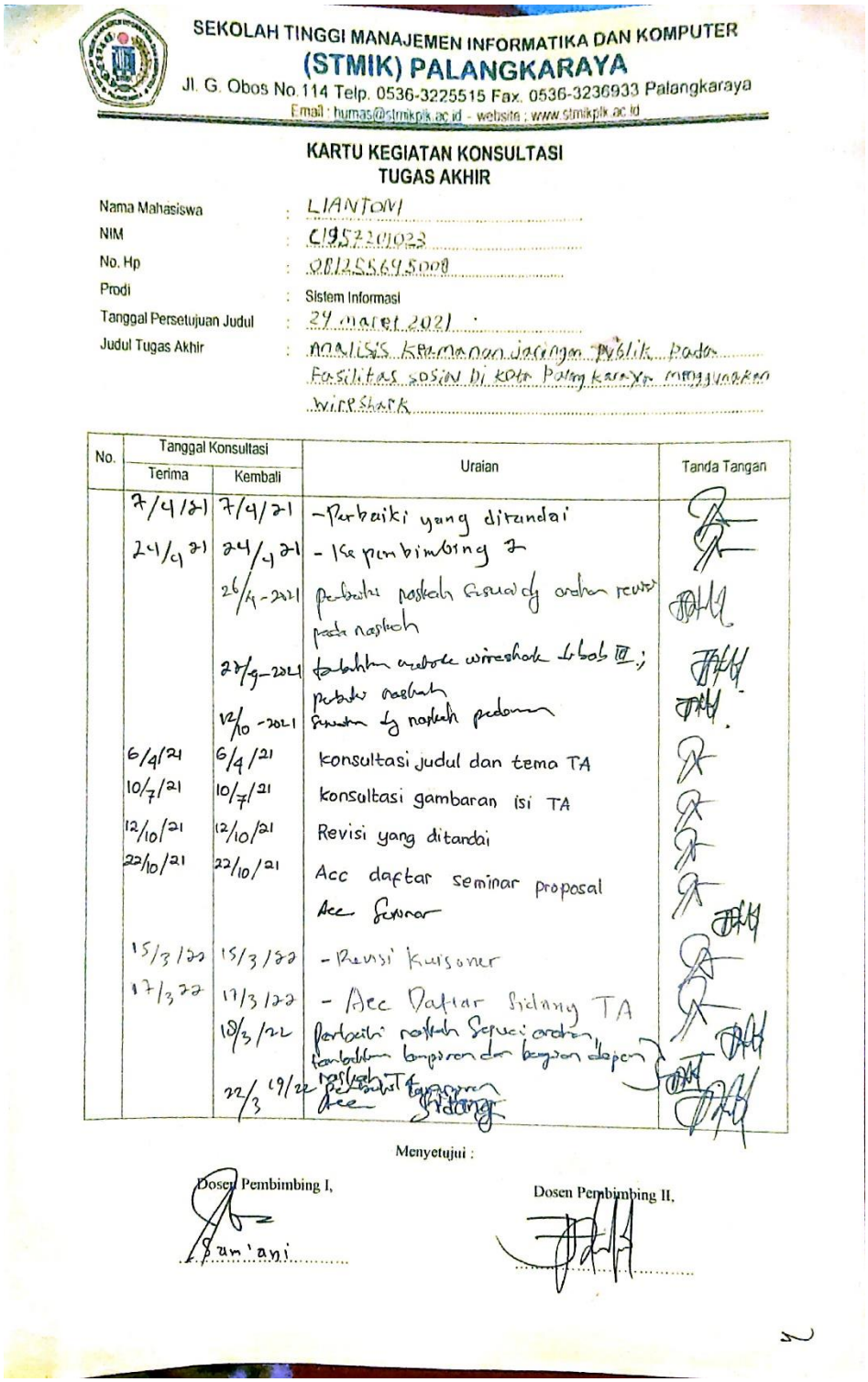
NIM : C1957201023

Demikian disampaikan dan dinyatakan mahasiswa tersebut di nyatakan telah melakukan penelitian dengan baik, atas perhatian dan kerjasamanya diucapkan terimakasih.

Plt. Kepala Dinas Komunikasi, Informatika, Statistik dan Persandian Kota Palangka Raya

Dra. FIFI ARFIANA, M.Si
Pembina Tingkat I
NIP. 19640704 198302 2 001

Lampiran 4. Kartu Kegiatan Konsultasi Tugas Akhir



SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp. 0536-3225515 Fax. 0536-3236933 Palangkaraya
Email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

KARTU KEGIATAN KONSULTASI TUGAS AKHIR

Nama Mahasiswa : LIANTONI
NIM : C1952201023
No. Hp : 082255695008
Prodi : Sistem Informasi
Tanggal Persetujuan Judul : 29 maret 2021
Judul Tugas Akhir : ANALISIS Keamanan jaringan Public pada Fasilitas sosial di kota Palangkaraya menggunakan wireshark

No.	Tanggal Konsultasi		Uraian	Tanda Tangan
	Terima	Kembali		
	7/4/21	7/4/21	-Perbaiki yang ditandai	
	24/4/21	24/4/21	- Ke pembimbing 2	
		26/4-2021	perbaiki naskah sesuai dg arahan revisi pada naskah	
		28/9-2021	tambahkan arahan wireshark bab III ; perbaiki naskah	
		12/10-2021	Sesuaikan dg naskah pedoman	
	6/4/21	6/4/21	konsultasi judul dan tema TA	
	10/7/21	10/7/21	konsultasi gambaran isi TA	
	12/10/21	12/10/21	Revisi yang ditandai	
	22/10/21	22/10/21	Acc daftar seminar proposal	
			Acc Seminar	
	15/3/22	15/3/22	- Revisi kuisoner	
	17/3/22	17/3/22	- Acc Daftar Sidang TA	
		18/3/22	perbaiki naskah sesuai arahan, tambahkan lampiran dan bagian depan	
		22/3/22	naskah perbaikan tanggapan Acc Sidang	

Menyetujui :

Dosen Pembimbing I,

Sum'ani

Dosen Pembimbing II,

Lampiran 5. Wawancara

LEMBAR WAWANCARA

A. Identitas

Nama : Dra. FIFI ARFIANA, Msi

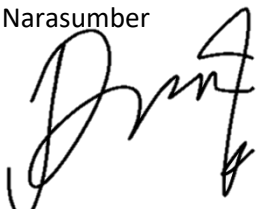
Jabatan : Pembina Tingkat 1

1. Apa masalah yang sering muncul saat jaringan wifi dipakai secara bersamaan? Jawaban: lambatnya internet terjadi ketika banyak orang di lingkungan sekitar, semuanya mencoba menggunakan koneksi internet pada saat yang bersamaan
2. Enkripsi apa yang digunakan untuk mengamankan jaringan Pada Pasuk Kameloh ini? Jawaban: Jenis Enkripsi yang dipakai untuk jaringan pasuk kameloh ini berjenis WPA2/PSK yang dengan autentikasi Pre-Shared Key
3. Apakah Anda menggunakan jaringan sebagai media komunikasi atau sebagai media penyimpanan data?

   Jawaban: Kedua-duanya sangat penting karena sangat membantu dalam memenuhi kebutuhan sehari-Hari, media komunikasi contohnya memberikan info-info penting seputaran Palangkaraya, media penyimpanan data penting menyimpan data secara online tidak perlu lagi kita membawa alat penyimpanan berupa hardisk atau flashdisk
4. Siapa saja yang dapat mengakses Jaringan wifi ini?

   Jawaban: orang umum dari muda sampai yang Tua bisa menikmati wifi gratis yang telah disediakan

Narasumber



Dra. FIFI ARFIANA, Msi

Lampiran 6. Jadwal Penelitian

No,	Rencana Kegiatan	September				Oktober				November				Desember					Januari				Febuari				Maret				April			
		I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV		I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
1.	Pengumpulan Kebutuhan																																	
2.	Konsultasi Dan Bimbingan																	2																
3.	Penulisan Proposal																	0																
4.	Seminar Proposal Tugas Akhir																	2																
5.	Perbaikan Proposal Tugas Akhir																	2																
6.	Penulisan Laporan Tugas Akhir																																	
7.	Membangun Prototype																																	
8.	Evaluasi Prototype																																	
9.	Pengkodean																	2																
10.	Pengujian Sistem																	0																
11.	Evaluasi Sistem																	2																
12.	Sidang Tugas Akhir																	2																
13.	Perbaikan Tugas Akhir																																	

Lampiran 7. Foto Wawancara

Lampiran 8. Lembar Kuesioner

LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	✓				
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan	✓				
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik	✓				
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif	✓				

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Fajar prayoga

LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan		✓			
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan		✓			
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik	✓				
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif	✓				

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Muhammad alifa rahmatulloh

LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	✓				
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan	✓				
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik	✓				
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif		✓			

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Henry Wijaya

LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	✓				
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan		✓			
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik	✓				
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif		✓			

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Widia

.....

LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	✓				
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan	✓				
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik	✓				
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif	✓				

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Putri aulia

LEMBAR KUESIONER

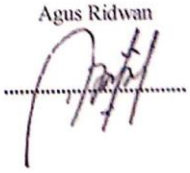
ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	✓				
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan	✓				
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik	✓				
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif		✓			

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Agus Ridwan



LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan		✓			
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan		✓			
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik		✓			
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif	✓				

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Sarah aurelia

LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	✓				
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan		✓			
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik	✓				
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif	✓				

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Darmo aji

.....

LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	✓				
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan	✓				
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik	✓				
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.		✓			
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif	✓				

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Ela fatimah

.....

LEMBAR KUESIONER

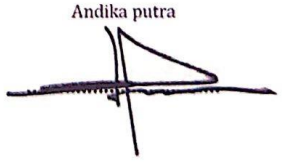
ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	✓				
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan	✓				
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik		✓			
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif		✓			

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Andika putra



LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	✓				
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan	✓				
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik	✓				
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif		✓			

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Muhammad fadli

LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program

No. Item	Pernyataan	Interval Jawaban				
		5 SB	4 B	3 CB	2 KB	1 STB
1	Apa jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan		✓			
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan		✓			
3	Kecepatan koneksi jaringan untuk mengakses google com sangat baik		✓			
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwidth yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif		✓			

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Risa Agus Pratama

LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	✓				
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan	✓				
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik		✓			
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif		✓			

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Novianto Bayu

LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan	✓				
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan	✓				
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik		✓			
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi		✓			
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif	✓				

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Hartanto

LEMBAR KUESIONER

ANALISIS KEAMANAN JARINGAN PUBLIK PADA FASILITAS SOSIAL DI KOTA PALANGKA RAYA MENGGUNAKAN WIRESHARK

Berilah tanda (✓) pada kolom nilai skor untuk memberikan penilaian terhadap program.

No. Item	Pernyataan	Interval Jawaban				
		5	4	3	2	1
		SB	B	CB	KB	STB
1	Apa Jaringan web server yang disediakan sangat stabil di setiap pengguna menggunakan		✓			
2	Delay yang terjadi pada jaringan sangat kecil dan tidak mengalami variasi penurunan kualitas jaringan	✓				
3	Kecepatan koneksi jaringan untuk mengakses google.com sangat baik	✓				
4	Layanan disediakan password mempermudah masyarakat dalam melakukan login kedalam jaringan wifi	✓				
5	Firewall efektif untuk mencegah serangan Hackers yang dapat merugikan masyarakat lain.	✓				
6	Bandwitdh yang digunakan saat ini sangat mencukupi bagi user untuk mengelola file gmail masing masing pengguna aktif	✓				

Keterangan:
5 = Sangat Baik
4 = Baik
3 = Cukup Baik
2 = Kurang Baik
1 = Sangat Tidak Baik

Andri Setiawan

.....