## ANALISIS KEAMANAN WEBSITE TERHADAP SNIFFING PROCESS PADA JARINGAN NIRKABEL MENGGUNAKAN APLIKASI WIRESHARK (STUDI KASUS : SIMAK UNISMUH)



# 105 82 1432 14

HASBULLAH JAMALUDDIN NURUL FITRIANI SUAEB 105 82 1405 14

PROGRAM STUDI TEKNIK TELEKOMUNIKASI JURUSAN TEKNIK ELEKTRO FAKULTAS TEKNIK UNIVERSITAS MUHAMMADIYAH MAKASSAR MAKASSAR 2018

## ANALISIS KEAMANAN WEBSITE TERHADAP SNIFFING PROCESS PADA JARINGAN NIRKABEL MENGGUNAKAN APLIKASI WIRESHARK (STUDI KASUS : SIMAK UNISMUH)

Skripsi

Diajukan sebagai salah satu syarat Untuk memperoleh gelar Sarjana Teknik Program Studi Teknik Telekomunikasi Jurusan Teknik Elektro Fakultas Teknik

Disusun dan diajukan oleh

HASBULLAH JAMALUDDIN 105 82 1432 14 NURUL FITRIANI SUAEB 105 82 1405 14

PADA UNIVERSITAS MUHAMMADIYAH MAKASSAR MAKASSAR

#### 2018



## UNIVERSITAS MUHAMMADIYAH MAKASSAR FAKULTAS TEKNIK

**GEDUNG MENARA IQRA LT. III** 

Jl. Sultan Alauddin No. 259 Telp. (0411) 866 972 Fax (0411) 865 588 Makassar 90221 Website : www.unismuh.ac.id, email : unismuh@gmail.com Website : http//teknik.unismuh.makassar.ac.id

د

HALAMAN PERSETUJUAN

Tugas Akhir ini diajukan untuk memenuhi syarat ujian guna memperoleh gelar Sarjana Teknik (ST) Program Studi Teknik Telekomunikasi Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Makassar

Judul Skripsi : ANALISIS KEAMANAN WEBSITE TERHADAP SNIFFING PROCESS PADA JARINGAN NIRKABEL MENGGUNAKAN APLIKASI WIRESHARK (STUDI KASUS : SIMAK UNISMUH)

NAMA

: 1. HASBULLAH JAMALUDDIN

2. NURUL FITRIANI SUAEB

STAMBUK

: 1. 105 82 1432 14 2. 105 82 1405 14

> Telah Diperiksa dan Disetujui Oleh Dosen Pembimbing

Pembimbing I

Pembimbing II

Dr. H. Zulfajri Basri Hasanuddin, M.Eng

Rahmania, ST.,MT

Mengetahui, Ketua Jurusan Teknik Elektro Dr. Umar Katu, ST.,MT NBM : 990410



## UNIVERSITAS MUHAMMADIYAH MAKASSAR FAKULTAS TEKNIK

**GEDUNG MENARA IQRA LT. III** 

Jl. Sultan Alauddin No. 259 Telp. (0411) 866 972 Fax (0411) 865 588 Makassar 90221 Website : www.unismuh.ac.id, email : unismuh@gmail.com Website : http//teknik.unismuh.makassar.ac.id

Makassar.

31

\_الله الحمر. د

#### PENGESAHAN

Skripsi atas nama HASBULLAH JAMALUDDIN dengan nomor induk Mahasiswa 10582143214 dan NURUL FITRIANI SUAEB dengan nomor induk Mahasiswa 10582140514, dinyatakan diterima dan disahkan oleh Panitia Ujian Tugas Akhir/Skripsi sesuai dengan Surat Keputusan Dekan Fakultas Teknik Universitas Muhammadiyah Makassar Nomor : 0005/SK-Y/20201/091004/2018, sebagai salah satu syarat guna memperoleh gelar Sarjana Teknik pada Program Studi Teknik Telekomunikasi Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Makassar pada hari Kamis tanggal 31 Mei 2018.

Panitia Ujian :

- 1. Pengawas Umum
  - a. Rektor Universitas Muhammadiyah Makassar Dr. H. Abd. Rahman Rahim, SE.,MM
  - b. Dekan Fakultas Teknik Universitas Hasanuddin

: Adriani, ST.,MT

Dr. Ir. H. Muhammad Arsyad Thaha, M.T

- 2. Penguji
  - a. Ketua

b. Sekretaris

: Andi Faharuddin, ST.,MT

- 3. Anggota
- : 1. Dr. Ir. Zahir Zainuddin, M.Sc-
  - 2. Rossy Timur Wahyuningsih, ST.,MT
  - 3. Dr. Umar Katu, ST.,MT

Mengetahui:

Pembimbing I

Dr. H. Zulfajri Basri Hasanuddin, M.Eng

Dekan ma

Ir. Hamzah Al Imran, ST.,MT NBM : 855 500 and the second

15 Ramadhan 1439 H

2018 M

Mei

.....

Pembimbing II

Rahmania, ST.,MT

#### KATA PENGANTAR

بير التحوير التحفير التحفير التحقيق

Assalamu'alaikum Warahmatullahi Wabarakatuh

Alhamdulillah, segala puji dan syukur penulis panjatkan ke hadirat Allah SWT. karena atas berkat dan rahmat-Nya penulis dapat menyelesaikan skripsi dengan judul "ANALISIS KEAMANAN WEBSITE TERHADAP SNIFFING PROCESS PADA JARINGAN NIRKABEL MENGGUNAKAN APLIKASI WIRESHARK (STUDI KASUS : SIMAK UNISMUH)". Tidak lupa pula penulis tuturkan shalawat serta salam kepada junjungan kita baginda Muhammad SAW., yang telah memberi suri tauladan atas umatnya.

Skripsi ini disusun guna melengkapi salah satu syarat untuk memperoleh gelar Sarjana Teknik pada Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Makassar. Skripsi ini dibuat berdasarkan pada data yang penulis peroleh selama melakukan penelitian, baik data yang diperoleh dari studi literatur, hasil percobaan maupun hasil bimbingan dari dosen pembimbing.

Penulis dapat menyelesaikan Skripsi ini, tidak lepas dari bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih yang sebanyak-banyaknya kepada:

- 1. Kedua orang tua serta keluarga yang telah memberikan bantuan baik berupa moril maupun materil.
- Bapak Ir. Hamzah Al Imran, S.T., M.T. selaku Dekan Fakultas Teknik Universitas Muhammadiyah Makassar.

- Bapak Dr. Umar Katu, S.T., M.T. selaku ketua Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Makassar.
- Bapak Dr. Eng. Ir. H. Zulfajri Basri Hasanuddin, M.Eng. selaku Pembimbing I dan Ibu Rahmania, S.T., M.T. selaku Pembimbing II yang telah memberikan waktu, arahan serta ilmunya selama membimbing penulis.
- Para Staff dan Dosen yang telah membantu penulis selama melakukan studi di Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Makassar.
- 6. Saudara-saudara serta rekan-rekan Vektor 2014 dan terkhususnya kelas Teknik Telekomunkasi yang telah banyak membantu penulis selama menyelesaikan studi dan skripsi ini.

Akhir kata penulis sampaikan pula harapan semoga Skripsi ini dapat memberi manfaat yang cukup berarti khususnya bagi penulis dan bagi pembaca pada umumnya. Semoga Allah SWT. senantiasa selalu memberikan rahmat dan hidayah-Nya kepada kita semua. Amiin.

Billahi Fi Sabilil Haq Fastabiqul Khairat Wassalamu'alaikum Warahmatullahi Wabarakatuh

Makassar, April 2018

Penulis

## ANALISIS KEAMANAN WEBSITE TERHADAP SNIFFING PROCESS PADA JARINGAN NIRKABEL MENGGUNAKAN APLIKASI WIRESHARK (STUDI KASUS : SIMAK UNISMUH)

Hasbullah Jamaluddin<sup>1</sup>, Nurul Fitriani Suaeb<sup>2</sup>

<sup>1,2</sup>Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Makassar E-Mail: <sup>1</sup><u>hasbuloke@gmail.com</u>, <sup>2</sup><u>suaebnurul@gmail.com</u>

#### ABSTRAK

Abstrak; Hasbullah Jamaluddin, Nurul Fitriani Suaeb; (2018); Perkembangan teknologi informasi khususnya di bidang jaringan komputer memungkinkan pertukaran informasi lebih cepat dan lebih kompleks dan data yang dipertukarkan dapat bervariasi. Pengguna internet dan penyedia jaringan nirkabel internet, memungkinkan mengakses apapun termasuk website dari manapun mereka mau, yang menyebabkan isu keamanan informasi menjadi penting. Proses penyadapan informasi (Sniffing) pada jaringan komputer menjadi semakin biasa dilakukan, baik untuk kegunaan yang bersifat positif maupun yang bersifat sebaliknya. Penelitian ini memberikan gambaran umum tentang keamanan website Simak Unismuh terhadap proses *sniffing* pada jaringan nirkabel, serta gambaran umum tentang kemungkinan metode serangan yang dapat terjadi pada website Simak Unismuh. Penelitian ini juga memberikan solusi kepada pengguna internet dan web developer untuk mencegah serangan dari kerentanan yang ditemukan. Dalam penelitian ini dilakukan dua tahap, yang pertama yaitu mengidentifikasi tingkat keamanan website Simak Unismuh menggunakan aplikasi Wireshark dan yang kedua yaitu membandingkan tingkat keamanan website Simak Unismuh dengan Google Account untuk mengetahui kelemahannya. Hasil dari penelitian ini adalah dengan penyerangan packet sniffing pada website Simak Unismuh, dapat merekam dan menampilkan informasi sensitif seperti username dan password dengan menggunakan aplikasi wireshark. Selain itu website Simak Unismuh rentan terhadap serangan MITM (man in the middle), karena belum menggunakan sertifikat SSL.

Kata Kunci: Keamanan Website, Sniffing, Jaringan Nirkabel, Aplikasi Wireshark.

### WEBSITE SECURITY ANALYSIS ON SNIFFING PROCESS ON WIRELESS NETWORK USING WIRESHARK APPLICATION (CASE STUDY: SIMAK UNISMUH)

Hasbullah Jamaluddin<sup>1</sup>, Nurul Fitriani Suaeb<sup>2</sup> <sup>1,2</sup>Department of Electrical Engineering, Faculty of Engineering, Muhammadiyah University of Makassar E-Mail: <sup>1</sup><u>hasbuloke@gmail.com</u>, <sup>2</sup><u>suaebnurul@gmail.com</u>

#### ABSTRACT

Abstract; Hasbullah Jamaluddin, Nurul Fitriani Suaeb; (2018); The development of information technology in general computer networks enables faster and more complex information exchange and interchangeable data may vary. Internet users and internet wireless network providers, allowing access to any website including from wherever they want to. Internet users and internet wireless network providers, allowing access to any website including wherever they want, which causes the issue of information security becomes important. The process of tapping the information (Sniffing) on computer networks becomes increasingly common, both for the use of a positive and the opposite. This study provides an overview of the security of Simak Unismuh website on the sniffing process on wireless networks, as well as an overview of possible attack methods that can occur on Simak Unismuh website. The research also provides solutions to Internet users and web developers to prevent attacks of vulnerabilities found. In this research, two stages are done, the first is to identify the security level of Simak Unismuh website using Wireshark application and the second is to compare the security level of Simak Unismuh website with Google Accounts to know the weakness. The result of this research is by attacking packet sniffing on Simak Unismuh website, can record and display sensitive information such as username and password by using wireshark application. In addition Simak Unismuh website vulnerable to MITM attacks (man in the middle), because they have not used the SSL certificate...

Keywords: Website Security, Sniffing, Wireless Networking, Wireshark Application.

#### DAFTAR ISI

HALAMAN SAMPUL		i
HALAMA	AN JUDUL	ii
HALAMA	HALAMAN PERSETUJUAN	
HALAMA	AN PENGESAHAN	iv
KATA PE	ENGANTAR	v
ABSTRA	Κ	vii
DAFTAR	ISI	ix
DAFTAR	GAMBAR	xii
DAFTAR	TABEL	XV
DAFTAR	DAFTAR LAMPIRAN	
DAFTAR SINGKATAN x		xvii
BAB I :	PENDAHULUAN	1
	A. Latar Belakang	1
	B. Rumusan Masalah	3
	C. Tujuan Penelitian	3
	D. Batasan Masalah	3
	E. Manfaat Penelitian	4
	F. Sistematika Penulisan	4
BAB II :	TINJAUAN PUSTAKA	6
	A. Website	6
	1. Web Server	6

	2. Database Server	8
	B. Form Processing PHP	8
	1. Atribut Action	8
	2. Atribut Method	9
	C. Protokol Jaringan	10
	1. TCP/IP	10
	2. IPX atau SPX	11
	3. NetBios	11
	D. Internet Layer atau Network Layer	11
	1. Transport Layer	11
	2. Application Layer	11
	3. TCP atau UDP <i>port</i>	12
	E. SSL dan TLS	13
	F. Aplikasi Wireshark	14
	G. Sniffing	16
	1. Passive Sniffing	16
	2. Active Sniffing	17
BAB III :	METODOLOGI PENELITIAN	18
	A. Waktu dan Tempat Penelitian	18
	1. Waktu Penelitian	18
	2. Lokasi Penelitian	18
	B. Teknik Pengumpulan Data	18
	1. Teknik Kepustakaan	18

	2. Teknik Observasi	18
	C. Teknik Analisis Data	18
	D. Kerangka Pemikiran	19
	E. Bahan dan Alat Penelitian	21
	F. Tahapan-tahapan Konfigurasi Software	21
	G. Teknis Pengujian Keamanan	22
BAB IV :	HASIL DAN PEMBAHASAN	31
	A. Analisis Hasil penelitian	31
	1. Skenario Pertama pada Website Simak Unismuh	31
	2. Skenario Kedua pada Website Google Account	38
	B. Pembahasan	44
	C. Solusi untuk Mencegah Serangan Packet Sniffing	47
BAB V :	PENUTUP	49
	A. Kesimpulan	49
	B. Saran	50
DAFTAF	R PUSTAKA	51
LAMPIRAN		53

#### DAFTAR GAMBAR

Gambar	Judul	Halaman
2.1	Web Server (Rerung, 2018)	7
2.2	Form Menggunakan GET (Rerung, 2018)	9
2.3	Hasil Proses Form Menggunakan Method GET (Rerung,	
	2018)	9
2.4	Form Menggunakan POST (Rerung, 2018)	10
2.5	Hasil Proses Form Menggunakan Method POST (Rerung,	
	2018)	10
2.6	Interface Grafis Pengguna Wireshark	12
3.1	Diagram Alir Penelitian	19
3.2	Topologi Jaringan Penelitian	22
3.3	Tampilan Awal Aplikasi Ettercap	23
3.4	Pemilihan Interface Jaringan	23
3.5	Tampilan Setelah Proses Scanning	24
3.6	Tampilan Daftar Hosts	24
3.7	Menambahkan IP Gateway sebagai Target 1	25
3.8	Menambahkan IP Korban sebagai Target 2	25
3.9	MITM Attack: ARP Poisoning	26
3.10	Memulai Proses Sniffing	26
3.11	Skema Lalulintas Data setelah MITM Attack : ARP	
	Poisoning aktif	27

3.12	Tampilan Awal Aplikasi Wireshark	27
3.13	Tampilan Interface Wlan0	28
3.14	Capturing Data pada Wlan0	28
3.15	Proses Login pada Website Unismuh	29
3.16	Google Chrome Menolak Koneksi	29
3.17	Browser Memberi Peringatan Keamanan	30
3.18	Menghentikan Proses Capturing	30
4.1	Hasil Rekaman Paket Data	32
4.2	IP address simak.unismuh.ac.id	33
4.3	Hasil Penyaringan Paket Data simak.unismuh.ac.id	33
4.4	Detail Paket Data TCP simak.unismuh.ac.id	34
4.5	Paket Data simak.unismuh.ac.id dengan Protokol HTTP	35
4.6	Detail Paket Data POST simak.unismuh.ac.id	36
4.7	Proses Komunikasi Data simak.unismuh.ac.id	38
4.8	IP address accounts.google.com	39
4.9	Hasil Penyaringan Paket Data accounts.google.com	40
4.10	Detail Paket Data TCP accounts.google.com	41
4.11	Paket Data accounts.google.com dengan Protokol TLS	42
4.12	Detail Paket Data Application Data accounts.google.com	43
4.13	Proses Komunikasi Data accounts.google.com	44
4.14	Proses Komunikasi Data Website Simak Unismuh	45
4.15	Proses Komunikasi Data Website Google Accounts	46
L1-1	Halaman Website Simak Unismuh	54

L1-2	Halaman Website Google Accounts	55
L2-1	Coloring Rules Wireshark	56
L2-2	Display Filter Wireshark	56
L3-1	Surat Permohonan Penelitian	57
L4-1	Melakukan Login pada Website Simak Unismuh dan	
	Google Accounts	58
L4-2	Menganalisis Paket Data yang Tertangkap pada Aplikasi	
	Wireshark	58

#### DAFTAR TABEL

Tabel	Judul	Halaman
2.1	Persyaratan Sistem Aplikasi Wireshark	15
2.2	Informasi Yang Dapat Diambil Dari Serangan Sniffing	17

#### DAFTAR LAMPIRAN

Lampiran	Judul	Halaman
1	Tampilan Halaman Website	54
2	Dialog Box sebagai Data Tambahan untuk Menganalisis	
	Paket Data pada Aplikasi Wireshark	56
3	Surat Penelitian	57
4	Dokumentasi Penelitian	58

#### DAFTAR SINGKATAN

Singkatan	Defenisi dan Keterangan
LAN	Local Area Network
URL	Uniform Resource Locator
WWW	World Wide Web
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Security
PHP	Hypertext Prepocessor
HTML	Hypertext Markup Language
ТСР	Transmission Control Protocol
UDP	User Datagram Protocol
FDDI	Fiber Distributed Data Interconnect
PPP	Point-to-Point Protocol
SLIP	Serial Line Internet Protocol
ATM	Asynchronous Transfer Mode
OS	Operating System
RAM	Random Access Memori
ROM	Read-only Memory
TELNET	Telecommunication network
POP	Post Office Protocol
IMAP	Internet Message Access Protocol
SMB	Server Message Block

FTP	File Transfer Protocol
MAC	Media Access Control Address
ARP	Address Resolution Protocol
SMTP	Simple Mail Transfer Protocol
IP	Internet Protocol
MITM	Man In The Middle
WLAN	Wireless Local Area Networks
DNS	Domain Name System
TLS	Transport Layer Security
SSL	Secure Socket Layer
СА	Certification Authority
ID	Identity
WPA	Wi-Fi Protected Access
PSK	Pre Shared Key

#### BAB I

#### PENDAHULUAN

#### A. Latar Belakang

Pada saat ini, kita hidup di zaman modernisasi. Zaman modernisasi biasanya ditandai dengan perkembangan teknologi, seperti munculnya berbagai teknologi baru dan lebih maju. Pada saat ini internet sangat berperan dalam kehidupan manusia. Dengan adanya internet, manusia dapat menemukan berbagai informasi dengan mudah. Di internet kita dapat melakukan berbagai hal, mulai dari mencari informasi, berkomunikasi dengan orang lain, transaksi jual beli dan lain sebagainya. Salah satunya dengan menggunakan *website*.

Hadirnya *website* sebagai sumber informasi dapat digunakan oleh suatu lembaga pendidikan untuk memberikan informasi yang mudah diakses seperti pada *website* Universitas Muhammadiyah Makassar. *Website* Unismuh dapat digunakan untuk keperluan aktivitas akademik dan menjadi akses membagikan informasi terkini seputar kampus unismuh, penerimaan mahasiswa baru, dan sistem informasi manajemen akademik. Penerapan sistem manajemen informasi pada *website* unismuh dapat memudahkan bagi mahasiswa untuk mendapatkan informasi seperti jadwal kuliah, tagihan, kartu rancangan studi, kartu hasil studi, dan transkrip nilai. Pada bagaian administrasi juga dimudahkan dengan adanya simak ini dalam mengolah data karena tidak perlu lagi berinteraksi dengan mahasiswa secara langsung. Dengan adanya simak ini juga dapat memudahkan dosen untuk mengolah data-data seperti nilai mahasiswa dan absensi. Untuk mengakses data-data pada simak Unismuh untuk *login* dengan cara memasukkan NIM dan kata kunci untuk mahasiswa, nomor identitas dan kata kunci untuk dosen, *user* dan kata kunci untuk staff.

Wireshark merupakan salah satu *network analysis tool*, atau disebut juga dengan *protocol analysis tool* atau *packet sniffer*. Wireshark dapat digunakan untuk *troubleshooting* jaringan, analisis, pengembangan *software* dan *protocol* serta untuk keperluan edukasi (Rosnelly & Pulungan, 2011). Wireshark dapat menangkap semua paket data yang lewat pada jaringan tanpa peduli kepada siapa paket itu dikirimkan. Disaat inilah biasanya terjadi pencurian data pribadi atau identitas oleh *hacker* jika tidak berhati-hati dalam beraktivitas di dunia maya. Data yang biasanya di incar adalah data yang cukup penting misalnya data akun, email, *username* dan *password*, dan lain-lain sehingga dapat merugikan orang-orang yang beraktivitas di dunia maya.

Berdasarkan hal tersebut, dengan maraknya tindak kejahatan pencurian data menggunakan media internet maka kami tertarik melakukan sebuah penelitian dengan judul "Analisis Keamanan Website terhadap Sniffing Process pada Jaringan Nirkabel Menggunakan Aplikasi Wireshark (Studi Kasus : Simak Unismuh)"

#### **B. Rumusan Masalah**

Rumusan masalah dari penulisan tugas akhir ini adalah sebagai berikut :

- 1. Apakah *website* Simak Unismuh aman terhadap proses *sniffing* pada jaringan nirkabel ?
- 2. Metode *sniffing* apa yang digunakan untuk melakukan penyerangan pada *website* Simak Unismuh ?
- 3. Apa yang sebaiknya dilakukan untuk mengamankan *website* Simak Unismuh dari serangan *sniffing* ?

#### C. Tujuan Penelitian

Tujuan dari penulisan tugas akhir ini adalah sebagai berikut :

- 1. Untuk mengetahui keamanan *website* Simak Unismuh terhadap proses *sniffing* pada jaringan nirkabel.
- Untuk mengetahui metode serangan *sniffing* yang digunakan pada *website* Simak Unismuh.
- 3. Untuk mengetahui cara mencegah serangan *sniffing* pada *website* Simak Unismuh.

#### D. Batasan Masalah

Untuk menghindari pembahasan yang meluas maka penulis akan membatasi masalah yang akan dianalisis yaitu :

 Penggunaan aplikasi Wireshark hanya untuk menganalisa keamanan website Simak Unismuh terhadap proses sniffing pada jaringan nirkabel serta membandingkan dengan salah satu website yang paling sering dikunjungi pengguna internet yaitu Google.

- Penulis hanya melakukan serangan *sniffing* pada *website* Simak Unismuh dan Google Account di Fakultas Teknik Universitas Muhammadiyah Makassar menggunakan jaringan nirkabel.
- 3. Penulis tidak melakukan implementasi peningkatan keamanan pada website Simak Unismuh dan hanya memberikan solusi yang sebaiknya dilakukan untuk mengantisipasi terjadinya serangan dari kerentanan yang di temukan seperti yang dilakukan penulis.

#### E. Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini adalah sebagai berikut :

- Sebagai data yang bisa diberikan dan digunakan oleh pihak IT Telekomunikasi Unismuh guna menjadi bahan pertimbangan dan masukan dalam upaya meningkatkan keamanan *website* yang lebih baik.
- 2. Meningkatkan pemahaman bagi pengguna layanan tentang bahaya *website* tanpa pengaman terhadap proses *sniffing* khususnya bagi pengguna yang awam terhadap bahaya *website* tanpa pengamanan.

#### F. Sistematika Penulisan

Sistematika penulisan tugas akhir ini akan dibahas dalam lima bab sebagai berikut :

#### BAB I : PENDAHULUAN

Bab ini terdiri dari latar belakang masalah, rumusan masalah, tujuan penenelitian, batasan masalah, manfaat penelitian, dan sistematika penulisan.

#### BAB II : TINJAUAN PUSTAKA

Landasan Teori berisi tentang teori-teori yang mendasari pembahasan secara detail, dapat berupa definisi-definisi atau model matematis yang langsung berkaitan dengan ilmu atau masalah yang diteliti.

#### BAB III : METODOLOGI PENELITIAN

Dalam bab ini diuraikan dengan gambaran objek penelitian, analisis semua permasalahan yang ada, dimana masalah-masalah yang muncul akan diselesaikan melalui penelitian yang dilakukan. Agar lebih sistematis, bab metode penelitian meliputi :

- 1. Waktu dan tempat penelitian.
- 2. Teknik pengumpulan data.
- 3. Teknik analisis data.
- 4. Kerangka pemikiran.
- 5. Bahan dan alat penelitian.
- 6. Tahapan-tahapan konfigurasi software.
- 7. Teknis pengujian keamanan.

#### BAB IV : HASIL DAN PEMBAHASAN

- 1. Hasil penelitian.
- 2. Analisa atau pembahasan.
- 3. Solusi untuk Mencegah Serangan Packet Sniffing.

#### BAB V : PENUTUP

- 1. Kesimpulan.
- 2. Saran.

#### **BAB II**

#### TINJAUAN PUSTAKA

#### A. Website

Situs web (bahasa Inggris: *website*) adalah suatu halaman web yang saling berhubungan yang umumnya berada pada peladen yang sama berisikan kumpulan informasi yang disediakan secara perorangan, kelompok, atau organisasi. Sebuah situs web biasanya ditempatkan setidaknya pada sebuah server web yang dapat diakses melalui jaringan seperti Internet, ataupun jaringan wilayah lokal (LAN) melalui alamat Internet yang dikenali sebagai URL. Gabungan atas semua situs yang dapat diakses publik di Internet disebut pula sebagai *World Wide Web* atau lebih dikenal dengan singkatan WWW (wikipedia.org, 2018).

1. Web Server

Web server adalah *software* yang menjadi tulang belakang dari *world wide web* (www). Web server menunggu permintaan dari *client* yang menggunakan *browser* seperti Netscape Navigator, Internet Explorer, Mozilla, dan program *browser* lainnya. Jika ada permintaan dari *browser*, maka web server akan memproses permintaan itu kemudian memberikan hasil prosesnya berupa data yang diinginkan kembali ke *browser*. Web server, untuk berkomunikasi dengan *client*-nya (*web browser*) mempunyai protokol sendiri, yaitu :

a. HTTP (hypertext transfer protocol)

Dengan protocol ini, komunikasi antar web server dengan *client*-nya dapat saling mengerti dan lebih mudah. Kata *Hyper Text* mempunyai arti

bahwa seorang pengguna internet dengan *web browser*-nya dapat membuka dan membaca dokumen-dokumen yang ada dalam komputernya atau bahkan jauh tempat sekalipun. Hal ini memberikan suatu proses yang *tridimensional*, pengguna internet dapat membaca dari satu dokumen ke dokumen yang lain hanya dengan mengklik beberapa bagian dari halaman-halaman dokumen (web) itu. Proses yang dimulai dari permintaan *webclient* (*browser*), diterima web server, diproses, dan dikembalikan hasil prosesnya oleh web server ke *web client* lagi dilakukan secara transparan (Rerung, 2018).



Gambar 2.1. Web Server (Rerung, 2018)

#### b. HTTPS (*hypertext transfer protocol secure*)

Merupakan protokol yang berorientasi terhadap keamanan pesan dalam suatu komunikasi. HTTPS dirancang agar dapat berdampingan dengan model pesan HTTP dan mudah diintergrasikan dengan HTTP dalam suatu jaringan. HTTPS menyediakan layanan keamanan yang dapat digunakan dengan bebas untuk kerahasiaan bertransaksi, *authenticity/integrity and nonrepudiability of origin* atau otentikasi dan keaslian maupun anti penyangkalan. Dalam impementasinya, HTTPS digunakan sebagai layanan keamanan pada suatu *website* yang memiliki data atau informasi yang bersifat rahasia baik yang dimiliki *user* maupun admin dari *website* tersebut. Suatu website yang menggunakan layanan HTTPS, dapat diketahui dengan adanya indikator ikon gembok pada *browser*, dan dapat terlihat pada *address bar* di *browser* dengan URL "https://" (Basri, 2015).

#### 2. Database Server

Database server merupakan suatu perangkat lunak yang mampu mengelola data dengan baik, sehingga data yang tersimpan dapat digunakan kembali. Database server menyediakan fleksibilitas untuk konfigurasi database service yang diinginkan. Client-server model dapat diartikan sebagai model dari suatu sistem yang membagi proses sistem antara server yang mengolah database dan client yang menjalankan aplikasi. Database server mengurangi beban akses data oleh client pada server. Database dapat diakses oleh beberapa client secara bersamaan dimana data yang diakses hanya diubah berasal dari satu sumber yaitu database pada server (Nazwita & Ramadhani, 2017).

#### **B.** Form Processing PHP

*Form* adalah fitur yang sangat penting dalam sebuah website. Hampir seluruh situs modern membutuhkan *form* sebagai fitur utama, seperti *form* pendaftaran, *form login, form* registrasi peserta, *form* pembayaran dan lain-lain. Untuk dapat memproses data dari *form*, membutuhkan perpaduan antara kode HTML dengan kode PHP. HTML digunakan untuk menampilkan *form*, sedangkan PHP digunakan untuk memproses *form* (Rerung, 2018).

#### 1. Atribut Action

Atribut action ini diisi dengan nilai berupa alamat halaman PHP dimana

akan diprosesnya *form* tersebut. Dalam contoh diatas, nilai action="proses.php", yang berarti menyediakan sebuah file dengan nama: proses.php untuk memproses *form* tersebut (Rerung, 2018).

#### 2. Atribut Method

Atribut method adalah atribut yang akan menentukan bagaimana cara form dikirim di dalam halaman proses.php. Nilai dari atribut method hanya bias diisi dengan satu dari dua pilihan, yakni GET atau POST. Method GET akan membuat nilai dari form yang akan dikirim melalui alamat URL website. Namun jika nilai method POST, maka nilai form tidak akan terlihat di alamat URL. Kelemahan paling jelas jika menggunakan method="get" adalah nilai dari form dapat dilihat langsung di dalam URL yang dikirim. Jika membuat form untuk data-data yang sensitif seperti password, maka form dengan method="get" bukan pilihan yang tepat (Rerung, 2018).



Gambar 2.2. Form Menggunakan GET (Rerung, 2018)





Keuntungan menggunakan method="post" dalam pemnuatan *form* PHP adalah bahwa isi dari *form* tidak ditampilkan di URL, sehingga *method* ini sesuai untuk data-data yang bersifat sensitif seperti *username* dan *password* (Rerung, 2018).



Gambar 2.4. Form Menggunakan POST (Rerung, 2018)



Gambar 2.5. Hasil Proses Form Menggunakan Method POST (Rerung, 2018)

#### C. Protokol Jaringan

Protokol didefinisikan sebagai prosedur dan pengaturan sejumlah operasi peralatan komunikasi data. Dalam komunikasi data, aturan-aturan meliputi cara membuka hubungan, mengirimkan paket data, mengkonfirmasi jumlah data yang diterima, dan meneruskan pengiriman data. Terdapat beberapa jenis protokol yang sering digunakan untuk mengimplementasikan sebuah jaringan (Yani, 2009).

#### 1. TCP/IP

TCP/IP (*Transmission Control Protocol-Internet Protocol*) merupakan protokol yang digunakan untuk jaringan internet. Protokol ini juga digunakan pada sistem operasi Unix-Linux (Yani, 2009).

#### 2. IPX atau SPX

IPX (Internetwork Packet eXchange) atau SPX (Sequence Packet eXchange) merupakan jenis protokol yang digunakan oleh Novell Netware yang pengaplikasiannya sering digunakan untuk multiplayer game (Yani, 2009).

3. NetBIOS

NetBIOS (*Network Basic Input-Output System*) merupakan jenis protokol yang digunakan oleh Microsoft untuk mengimplementasikan *Local Area Network* (LAN) *manager* (Yani, 2009).

#### **D.** Internet Layer atau Network Layer

1. Transport Layer

Dua protokol yang bekerja pada layer ini adalah TCP (*Transmission Control Protocol*) dan UDP (*User Datagram Protocol*). TCP memberikan *service connection oriented*, *reable*, dan *byte stream service*. Penjelasan mengenai servis tersebut lebih kurang sebagai berikut. Sebelum melakukan pertukaran data seriap aplikasi menggunakan TCP, diwajibkan membentuk hubungan (*handshake*) terlebih dahulu. Kemudian, dalam proses pertukaran data, TCP mengimplementasikan proses deteksi kesalahan paket dan re-transmisi dan semua proses terrnasuk pengiriman paket data ke tujuan secara berurutan (Yani, 2009).

2. Application Layer

Di dalam model OSI, lapisan aplikasi menyediakan jasa untuk suatu program aplikasi yang bertujuan agar komunikasi efektif dapat terjadi dengan program aplikasi lain di dalam jaringan. Lapisan aplikasi bukanlah aplikasi itu sendiri, melainkan suatu layanan yang menyediakan jasa seperti berikut.

- a. Meyakinkan bahwa pihak lain dapat dikenali dan bisa dicapai.
- b. Membuktikan keaslian, baik pada pengiriman pesan maupun saat penerimaan, ataupun keduanya sekaligus.
- c. Memastikan sumberdaya komunikasi yang ada.
- d. Memastikan persetujuan pada akhir keduanya, tentang prosedur perbaikan kesalahn, dan integrasi data.
- e. Menentukan protokol dan sintaksis data pada tingkatan aplikasi (Yani, 2009).
- 3. TCP atau UDP Port

Port adalah pintu dari suatu node IP untuk menerima dan mengirim data. Port dimulai dari 0 sampai 65536. Port 0-1024 disebut well known port atau port yang sudah dikenal dan telah melewatu proses standarisasi. Contoh port TCP sebagai berikut

- FTP : *Port* 20/21
- Telnet : Port 23
- SMTP : *Port* 25
- POP3 : *Port* 110
- HTTP : *Port* 80

Contoh port UDP sebagai berikut.

- Netstat : Port 15
- DNS : *Port* 53
- Netbios : *Port* 137 (Yani, 2009).

#### E. SSL dan TLS

Secure Socket Layer (SSL) dan Transport Layer Security (TLS), merupakan kelanjutan dari protokol kriptografi yang menyediakan komunikasi yang aman di Internet. Protokol ini menyediakan authentikasi akhir dan privasi komunikasi di Internet menggunakan *cryptography*. Dalam penggunaan umumnya, hanya server yang diauthentikasi (dalam hal ini, memiliki identitas yang jelas) selama dari sisi *client* tetap tidak terauthentikasi. Authentikasi dari kedua sisi (mutual authentikasi) memerlukan penyebaran PKI pada *client*-nya. *Protocol* ini mengizinkan aplikasi dari *client* atau server untuk berkomunikasi dengan didesain untuk mencegah *eavesdropping*, *tampering*, dan *message forgery*. Baik TLS dan SSL melibatkan beberapa langkah dasar :

- Negosiasi dengan ujung *client* atau server untuk dukungan algoritma.
- Public key, encryption-based-key, dan certificate-based authentication.
- Enkripsi lalulintas symmetric-cipher-based.

Protocol SSL dan TLS berjalan pada layer di bawah application protocol seperti HTTP, SMTP and NNTP dan di atas layer TCP transport protokol, yang juga merupakan bagian dari TCP/IP protocol. Selama SSL dan TLS dapat menambahkan keamanan ke protocol apa saja yang menggunakan TCP, keduanya terdapat paling sering pada metode akses HTTPS. HTTPS menyediakan keamanan web-pages untuk aplikasi seperti pada Electronic commerce. Protocol SSL dan TLS menggunakan cryptography public-key dan sertifikat publik key untuk memastikan identitas dari pihak yang dimaksud. Sejalan dengan peningkatan jumlah client dan server yang dapat mendukung TLS atau SSL alami, dan beberapa masih belum mendukung. Dalam hal ini, pengguna dari server atau *client* dapat menggunakan produk *standalone*-SSL seperti halnya Stunnel untuk menyediakan enkripsi SSL (wikipedia.org, 2018).

Dalam penerapan terhadap suatu proses HTTPS di jaringan internet, keterlibatan pihak ketiga sangat diperlukan. Hal ini karena, harus adanya suatu pihak yang dapat menjamin terhadap keaslian suatu web-server dalam arti bahwa yang sedang diakses oleh client merupakan website yang sah atau dalam kriptografi dikenal dengan istilah authentication baik terhadap entity authentication atau identitas dari pihak yang berkomunikasi, data, public key dll. Pihak ketiga/ pihak terpercaya, dalam kasus ini adalah certification authority (CA), memiliki tugas, diantaranya: "Mengeluarkan certificate, menyediakan dan menjamin otentikasi *public key* suatu pihak. Dalam sistem berbasis sertifikasi hal ini termasuk mengikat public key pada nama-nama yang berlainan melalui sertifikat yang telah disahkan, mengelola nomor-nomor seri sertifikat dan penarikan/pembatalan sertifikat" (Basri, 2015).

#### F. Aplikasi Wireshark

Wireshark adalah alat penganalisis paket jaringan *open source* yang menangkap paket data yang melewati jaringan dan menyajikannya dalam bentuk yang dapat dimengerti. Wireshark dapat dianggap sebagai pisau tentara Swiss karena dapat digunakan dalam situasi yang berbeda seperti masalah jaringan, operasi keamanan, dan protokol pembelajaran internal. Wireshark mendukung berbagai protokol mulai dari TCP, UDP, dan HTTP ke protokol canggih seperti AppleTalk (Singh, 2013).

Wireshark dapat membaca data secara langsung dari *Ethernet*, *Token-Ring*, FDDI, *serial* (PPP and SLIP), 802.11 *wireless* LAN , dan koneksi ATM. *Tools* ini bisa menangkap paket-paket data/informasi yang berjalan dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang *tool* ini juga dapat dipakai untuk *sniffing* (memperoleh informasi penting seperti *password* email atau *account* lain) dengan menangkap paket-paket yang berjalan di dalam jaringan dan menganalisanya. Untuk struktur dari *packet sniffer* terdiri dari 2 bagian yaitu *packet analyzer* pada *layer application* dan *packet capture* pada *layer operating system* (Dewi, Rimra, & Vitria, 2012). Untuk menjalankan aplikasi Wireshark diperlukan persyaratan sistem sebagai berikut.

Feature	Description
OS	Windows <i>any version</i> , Apple macOS, Linux, Solaris, FreeBSD, NetBSD, <i>any other</i> .
Processor	<i>Any modern</i> 64-bit AMD64/x86-64 or 32-bit x86 <i>processor</i> .
RAM	400 MB available RAM.
ROM	300 MB available disk space.
Resolution	1024 x 768 (1280 x 1024 or higher recomrnded).
Network card for capturing	Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, <i>and other</i> .

Tabel 2.1. Persyaratan Sistem Aplikasi Wireshark.

Sumber : wireshark.org (2018).



Gambar 2.6. Interface Grafis Pengguna Wireshark.

#### G. Sniffing

Sniffing dalam pengertian berarti mengendus, sedangkan dalam ilmu keamanan jaringan sniffing merupakan aktifitas menangkap paket-paket data yang lewat dalam sebuah jaringan. Sniffing sendiri biasanya digunakan untuk menangkap informasi - informasi vital dari sebuah jaringan seperti password, email text, dan File transfer. Sniffing biasanya menyerang protokol-protokol seperti Telnet, HTTP, POP, IMAP, SMB, FTP, dan lain-lain. Dalam metode hacking, sniffing dibagi menjadi dua bagian yaitu passive sniffing dan active sniffing (Hamid, 2017).

1. Passive Sniffing

*Passive sniffing* merupakan aktifitas *sniffing* yang dilakukan pada jaringan dengan media penghubung *hub*. Dimana *hub* akan melakukan *broadcast* seluruh paket yang melewatinya ke seluruh *node* yang terhubung ke *hub* tersebut. *Hub* merupakan perangkat komputer yang melakukan *broadcast* paket data ke seluruh

jaringan sehingga *sniffing* pada jaringan dengan *hub* sangat mudah dilakukan (Hamid, 2017).

#### 2. Active Sniffing

Active sniffing merupakan aktifitas sniffing yang dilakukan pada jaringan dengan media penghubung switch atau sejenisnya. Switch sendiri merupakan sebuah perangkat penghubung yang memiliki chip untuk menyimpan tabel MAC address. Switch tidak lagi mem-broadcast paket ke seluruh jaringan namun paket data yang dikirim hanya melalui port asal dan port tujuan saja. Sehingga sangat sulit untuk melakukan sniffing pada switch. Diperlukan metode khusus untuk melakukan sniffing pada switch. Untuk melakukan sniffing pada jaringan dengan switch perlu membuat membanjiri media penyimpanan pada switch dengan MAC address sehingga switch tersebut tidak ada bedanya dengan hub. Untuk membanjiri media penyimpanan dapat menggunakan ARP poisoning ataupun MAC Flooding (Hamid, 2017).

No	Protokol	Informasi Yang di Dapat
1	TELNET	Key stroke
2	HTTP	Data sent in clear text
3	SMTP	Password and data sent in clear text
4	NNTP	Password and data sent in clear text
5	POP	Password and data sent in clear text
6	FTP	Password and data sent in clear text
7	IMAP	Password and data sent in clear text
8	SMB	Data sent

Tabel 2.2. Informasi Yang Dapat Diambil Dari Serangan Sniffing.

Sumber : Hamid (2017).

#### **BAB III**

#### METODOLOGI PENELITIAN

#### A. Waktu dan Tempat Penelitian

1. Waktu Penelitian

Adapun waktu kegiatan penelitian yang dilakukan dimulai pada bulan April 2018 sampai semua proses pengumpulan data selesai.

2. Lokasi Penelitian

Lokasi pengambilan data pada penelitian ini dilakukan di Fakultas Teknik Universitas Muhammadiyah Makassar.

#### **B.** Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini adalah sebagai berikut :

1. Teknik Kepustakaan

Teknik kepustakaan dilakukan dengan melakukan pengumpulan materimateri yang berkaitan dengan keamanan *website* yang berasal dari buku, jurnal dan hasil *browsing* di internet.

2. Teknik Observasi

Teknik observasi dilakukan pada 2 *website* yaitu *website* Simak Unismuh dan *website* Google Accounts. Namun pada penelitian ini kami memilih *website* Simak Unismuh sebagai objek utama.

#### C. Teknik Analisis Data

Data-data hasil observasi dengan aplikasi Wireshark yang diperoleh kemudian dianalisis untuk mendapatkan hasil dengan cara
membandingkan keamanan *website* Simak Unismuh dan *website* Google Accounts terhadap proses *sniffing* pada jaringan nirkabel.

# D. Kerangka Pemikiran

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





Gambar 3.1. Diagram Alir Penelitian

Sesuai dengan diagram alir penelitian pada Gambar 3.1, penelitian ini dilakukan dalam beberapa tahapan.

- 1. Mengumpulkan dan mempelajari literatur, buku-buku, *ebook* dan artikel untuk menunjang penelitian.
- 2. Menyiapkan *hardware* dan *software* yang dibutuhkkan untuk menunjang pelaksanaan penelitian.
- Melangkah untuk melakukan sebuah percobaan serangan *sniffing* pada *website* Simak Unismuh dan Google Accounts menggnakan aplikasi Wireshark untuk mendapatkan informasi tentang keamanannya.
- 4. Menganalisis data yang diperoleh dari kedua percobaan serta membandingkan tingkat keamanan *website* Simak Unismuh dan *website* Google Accounts terhadap proses *sniffing*.
- 5. Menarik kesimpulan untuk memutuskan sebuah saran yang bisa digunakan untuk mengamankan *website* terhadap proses *sniffing* melihat dari sisi pengguna.

#### E. Bahan dan Alat Penelitian

Dalam penelitian ini bahan penelitian berdasarkan dari teori dasar keamanan *website* yang diambil dari berbagai literatur seperti buku, jurnal, artikel berbentuk *softcopy* dan *hardcopy*. Untuk spesifikasi alat yang digunakan penelitian adalah sebagai berikut :

- 1. Kebutuhan perangkat keras dan sistem operasi.
  - Laptop Acer E1-471, Prosesor Intel Core i3-2348 2.30 GHz, RAM 2 GB.
  - Wireless Network Card Atheros 802.11b/g/n.
  - Sistem operasi Kali Linux 64bit.
  - Smartphone android Xioami Redmi 4X (sebagai Hotspot).
  - Smartphone android Samsung Grand Prime (Sebagai Target).
- 2. Kebutuhan perangkat lunak.
  - Software Wireshark (untuk serangan packet sniffing).
  - Software Ettercap (untuk serangan poisoning).

## F. Tahapan-tahapan Konfigurasi Software

- 1. Konfigurasi Ettercap
  - Membuka terminal kemudian mengetik perintah "#gedit /etc/ettercap/etter .conf" maka akan muncul tampilan seperti gambar berikut.
  - Mengubah nilai "ec\_uid = 0" dan "ec\_gid" = 0
  - Menghilangkan tanda taggar didepan "iptables"
  - Menyimpan hasil konfigurasi.

# G. Teknis Pengujian Keamanan

Sebelum penelitian diimplementasikan, perlu dibangun sebuah perencanaan yang nantinya membantu memudahkan jalannya proses pelaksanaan identifikasi pada penelitian. Kegiatan ini biasanya disebut sebagai analisa desain topologi (*topology design*).

Pada analisa ini terlibat komponen perangkat yang saling berhubungan, yaitu: jaringan internet, wifi *hotspot* yang bersal dari *smartphone*, laptop penyerang dan *smartphone* target. Untuk lebih jelasnya dapat dilihat pada gambar berikut.



Gambar 3.2. Topologi Jaringan Penelitian

Setelah mengetahui skema yang ditunjukkan pada Gambar 3.9, maka langkah selanjutnya yaitu pengujian keamanan bertujuan untuk memperoleh kesadaran akan permasalahan keamanan pada *website* yang dikunjungi.

- 1. Mengkoneksikan laptop dengan sebuah jaringan internet. Dalam kasus ini penulis menggunakan *hotspot smartphone* android.
- 2. Membuka Ettercap, pada Kali Linux pilih "*Aplications*" kemudian "*Sniffing & spoofing*" lalu pilih "Ettercap". Maka akan muncul *interface* Ettercap seperti yang terlihat pada gambar berikut.



Gambar 3.3. Tampilan Awal Aplikasi Ettercap

3. Mengklik menu "*Sniff*" kemudian klik "*Unified sniffing*" dan pilih *interface* yang akan digunakan. Dalam kasus ini penulis menggunakan *interface* wlan0 seperti yang terlihat pada gambar berikut.



Gambar 3.4. Pemilihan Interface Jaringan

4. Meng-scan host yang ada di dalam jaringan dengan cara mengklik menu "Hosts" kemudian pilih "Scan for hosts" lalu tunggu sampai proses scanning selesai. Setelah proses scanning selesai maka akan terlihat jumlah host yang terhubung pada jaringan yang sama dengan penyerang.



Gambar 3.5. Tampilan Setelah Proses Scanning

Pada Gambar 3.5 terdapat 2 hosts yang terhubung pada jaringan yang sama.

5. Melihat daftar *host* yang telah di-*scan* dengan cara mengklik menu "*Hosts*" kemudian pilih "*Host list*", maka akan muncul daftar *host* seperti gambar berikut.

			ettercap 0.8.2		0	0
Start Targets H	Hosts View Mitm	Filters Logging	Plugias Info			
l lost List ×						
IP Address	MACAddress	Description				
192.158.43.1	4C:49:E3:B1:54:7D					
192.158.43.121	8C:BF:A6:5B:E1:21					
D	elete Host		Add to Target 1	Acd to Target	2	
Lua: no scripts we	ere specified, not sta	rtine up				4
Starting Unified s	niffing	2.1				
Randomizing 255	hosts for scanning					
Scapping the who	le netroack for 2551	haete				
Scanning the who 2 hosts added to	le netmask for 255 l the hosts list	hasts				ł

Gambar 3.6. Tampilan Daftar Hosts

6. Untuk melakukan ARP *poison*, pertama yang dilakukan adalah menentukan *gateway* dan target dengan cara melihat IP *address*-nya. Selanjutnya yaitu menambahkan IP Address 192.168.43.1 sebagai Target 1 dengan cara mengklik alamat IP tersebut kemudian pilih "*Add to Target* 1". Karena IP *address* tersebut merupakan IP address *gateway*.

						etterca	0.8.2				0	•	0
Start Targets	losts	view	Mitm	Filters	Logging	Flugins	Info						
lost List ×													
IP Address	MACA	odres	ç	Descri	ption								
192.168.43.1	4C.49	C3 61	54 7D	8									
2	Delete H	ast				Add to T	arget 1		Ac	to Targ	get 2		
ue: no scripts v	Delete H were spec	ost iñed,	not sta	arting up	21	Add to T	anget 1		Ac	i to Tarj	get ?		

Gambar 3.7. Menambahkan IP Gateway sebagai Target 1

 Selanjutnya menambahkan IP Address 192.168.43.121 sebagai target 2 dengan cara mengklik alamat IP kemudian pilih "*Add to Target* 2". Karena IP tersebut merupakan IP *address* korban.

					etterca	ip 0.8.2				0	٠	0
Start Targets	Hosts Vie	w Mitm	Filters	Logging	Plugins	Info						
last i lst ×												
IP Address	MAC Acd	ress	Descrip	otion								
192.168.43.1	40:49:53	B1:54:7D										
192,168 43 12	1 8C:BF:AG	58 EI 21	-									
	N.I.da Kara				Sold in 1	Lunul 1		S-del in	Tours ?	-		
1	Delete Host	8			Add to 1	larget 1		Add lu	(Target )	2		
Lurting Unified	Delete Host	2			Add to 1	larget 1		Add to	Target a	ź		
L Larling Unified :	Detete Host				Add to 1	larget 1		Add to	• Target 3	2		
L Larting Unified : andomizing 251	Detete Host sniffing 5 hosts for s	cenning.	[_		Add to 1	larget 1		Add to	) Target 3	2		
Larling Unified andomizing 25 canning the wh	Detete Host sniffing o hosts for s tote notmas	conning k for 255	hosts		Add to 1	larget 1		Add to	) Target 2	2		
Larting Unified : andomizing 25 canning the wh hosts added to cost 192 168 43	Detete Host snilling o hosts for s tote netmas i t the hosts i t added to	canning k for 255 ist TARSET	hosts		Add to 1	largel 1		Add lo	) Target 3	2		

Gambar 3.8. Menambahkan IP Korban sebagai Target 2

8. Menjalankan ARP *poisoning* dengan cara mengklik menu "Mitm" kemudian memilih "ARP *poisoning*" lalu centang "*Sniff remote connection*".

Host List *			
P Address MAC Address Desc	rption		
192.168.43.1 4C.49.E3.81:54:70			
192.158.43.121 8C/BF:A5:5B/C1:21			
	Optional parameters     Soff nemote connections     Only poison one way.     Cancel		
Delet: Host	Add to Target 1	Add to Target 2	
meanizing 255 hosts for scanning canning the whole netmask for 255 hosts hosts acide to the hosts list ost 192.168.43.1 acced to TARGET1			

Gambar 3.9. MITM Attack: ARP Poisoning

9. Mengklik "Ok", Kemudian menjalankan *sniffing* dengan cara mengklik menu

"Start" kemudian pilih "Start sniffing".

Start         Targets         Hosts         View         Mitm         Filters         Logging         Plugins         Info           Stop snifting         Shift+Ctil+E         Description         Description			
Start snifting         Shift+Ct-I+W           Stop snifting         Shift+Ct-I+E           Description         Exit           Exit         Ct-I+Q 70           102:168.43.121         8C:BF:A6:58/E1:21           Detete Host         Add to Target 1         Add to Target 1			
Stop snifting     Shift+Ct/LE     Description       Ext     Ct/L-Q 7D       192 168.43.121     6C:BP:A6/SB E1:21       Detete Host     Add to Target 1       Add to Target 1     Add to Target 1			
Det Cet+Q 7D 192 168,43 121 8C/8F:A658/E1-21 Detete Host Add to Target 1 Add to Target 1 Add to Target			
192 168.43.121 &C:BF:A6:5B:E1:21 Defecte Host Add to Target 1 Add to Target 1 Add to Target 1			
Delete Host Add to Target 1 Add to Target			
Delete Host Add to Target 1 Add to Target			
Delete Host Add to Target 1 Add to Target			
Delete Host Add to Target 1 Add to Target			
Delete Host Add to Target 1 Add to Target 1 Add to Target			
Delete Host Add to Target 1 Add to Target 1 Add to Target			
Detete Host Add to Target 1 Add to Target 1			
Delete Host Add to Target 1 Add to Target			
	2	_	-
RP naisonairea via litera			
ni pasaning recurs.			
SRCUP 1 : 192.168.43.1 4C:49:E3:B1:54:7D			
			1
3ROUP 2 : 192.168.43.121 8C:BF:A6:5B:E1:21			

Gambar 3.10. Memulai Proses Sniffing

Setelah MITM *Attack* : ARP *Poisoning* aktif maka proses pengiriman data dari *smartphone* target menuju *hotspot* atau sebaliknya akan melewati laptop penyerang. Skemanya sebagai berikut.



Gambar 3.11. Skema Lalulintas Data setelah MITM *Attack* : ARP *Poisoning* aktif 10. Membuka Wireshark, pada Kali Linux pilih "*Aplications*" kemudian "*Sniffing* 

& *spoofing*" lalu pilih "Wireshark", maka akan muncul tampilan awal aplikasi Wireshark seperti gambar berikut.

	The Wireshark Network Analyzer		
$ \begin{tabular}{lllllllllllllllllllllllllllllllllll$	Wireless Tools Help		
4 E 4 8 6 7 8 7 6 8 5 E 1			
Apply a deptay filter _ <ctd-as< td=""><td></td><td></td><td>💽 🕴 Promission . 🛛 🔸</td></ctd-as<>			💽 🕴 Promission . 🛛 🔸
Welcome to Wireshark			
Capture			
	S.	- All interfaces shown -	
Wind	18		
411	1		
Loophtck lo	-		
ellio			
ricas	-		
ushmon ]	-		
usbmcn2			
@ Osco remote captures cisco	-		
Random packet generator: randokt			
@ SSH remote capture: ssh			
iss open pitterer remote capture, scipture	P		
Learn			
CLUIN			
User's Guide Wiki - Questions and A	Answers Meiling Lists		
You are running Wireshark 2.4.3 (Git v2.4.	3 packaged as 2.4.3-1).		
7 Reads to load or capture		No Fackets	Profile: Default

Gambar 3.12. Tampilan Awal Aplikasi Wireshark

11. Kemudian masuk ke dalam *interface* yang memiliki paket data pada jaringan yang ditandai dengan adanya diagram gelombang. Pada kausus ini penulis

akan masuk pada interface Wlan0 dengan cara mengklik dua kali pada *interface*.

				Capturing from wlan0		000
<u>Bis</u> E	cilt ⊻lew <u>G</u> o	Capture Analyze Sta	itistics Telephony <u>Wireless</u> <u>T</u> oo	k <u>H</u> elip		
	1 🕥 P	PBBC	* * .) !* * 🚍 🧮	a a a II		
A200	y a display tiller	«Ctri-//>				Expression. +
No.	Time	Source	Destination	Protocol Length Info		
*						
-						
0.5	wahtt: klive.ca	pture in progress>			No Packets	Profile: Default

Gambar 3.13. Tampilan Interface Wlan0

12. Setelah masuk kedalam *interface* maka aplikasi Wireshark secara otomatis akan men-*capture* data yang lewat pada jaringan Wlan0.

	000	X C Q + +			. 旺	
E Annio	t display filter of	ret. as	-			Incarrow 1
	a contract of the second					Expression.
20.	time	Source	Distinition	Protoco	Longth Into	
	10.00000000	102,108,45,161	00.80.04.122	700	66 54726 88 [AUN] 50051 ACK	-1 WIN-255 LCH-0 ISWal-37390 SCCP-8287640
	2 0.000091428	182.198.10.121	30.89.34.122	TCP	00 03721 - 00 [ACK] 340-1 ACK	-1 WIN-183 Len-0 15Wal-3,390 Sect-826/04/
	0.000100170	192.108.40.121	00.00.00.126	TCD	tand an angent facul des a Aus	4254000000 WIN 402 Lon 0 avai 3.400 Tacc
	E 0.000324400	30.08.04.122	102,100,40,121	TOP	1404 86 - 03721 [//CK] 860 1 //CK	1240 dated th and 2 temperat 526/04/ 1360/ 3735
	5 0.006149032	30.03.31.144	102 160 42 121	TCP	65 66 - 53731 [Far, ACK] 580-	1 2-4-1 din-228 1 mm 0 75m -8207660 75mm-27
	7.0.002008260	103 169 10 971	25 80 64 122	TER	65 69795 . SO [SCH] Sonra Kov	-1 WIT-192 Lan-B TEMS -27988 TEAST-2798 TEAST
	7 0.003023203	102,100,+5,121	0010010001222	100		THE HOS LET & ISVAL STORE SECTOR
	3 0 004903130	162 148 43 121	25 80 54 122	TCP	65 53731 - 99 [ACK] Sec-1 Are	-1380 Min-505 Leg-0 TSus1-37300 TSust -828764
	13 R 004960853	102 168 48 121	35 R0 54 122	TCP	66 59721 - 88 [ACK] SCOTT 6CK	1763 Win=527 Lenze TSwa1=37398 TScor=828764
	11.6.005662122	26.86.64.122	192 168 43 121	TCP	66.86 53723 [FTK 4CK] Spore	1 Ankol Winc235 Lence TSvalc8287656 TScorc37.
	12.0.005000707	36.09.54.122	192, 188, 43, 121	1022	BE HE - STUDY DOLL ACRE SPOR	1 Ackel winezas Leneo Isvalesznysso isdorea/
	13.0.005203356	36 80 64 122	102 168 43 121	TCP	65.86 53725 ICTN, ACKT SPOR	1 Anka1 wina235 (ream) TSvalas287651 TScora37
	14 0 005/101/1	26 119 54 122	192 158 43 121	TEP	55 DE - 52772 [FIN ACA] SPOR	1 Ackel wine235 Lenge 15vale8280656 ISected/
	15 0.007051575	192,168,43,121	35,89,54,122	1CP	BE 53/21 - BU [ACE] SCOPT ACK	=2 win=123 Lenep (Swales/200) [Secrem20/050
	15 6.009116544	192.168.43.121	35,89,54,122	TCP	65 53721 - 68 [ACK] Seg=1 Ack	=1389 Win=585 Len=0 TSval=37398 TSecr=828764
	1/ 0 009334104	192.168.43.121	35,89,54,122	TCP	65 53721 - UO [ACH] SEGRI ACK	#1/53 Min#527 Len#0 [Sva]#3/390 [Secr#020/64
	18 8.089485343	36.88.54.172	192-108-43-121	TCP	65 [TCP Recransmissing] 58 -	53723 [FIN, ACK] Seg=1 Ack=1 Win=285 Len=6 T
	2.5. A. (600/233320	HACTOR BALANCE	455-389-57 195-		PP TPD Deservation and PD	PAYIN PPTH. THUI Paper taket Handhill Paper
Eche Inte Tran	rnet II, Sros L rnet Protocol V smission Contro 4c 49 e3 b1 54	iteonTe 10:56:79 (2 ersion 4, Src: 192. 1 Protocol, Src Per 7d 2c d6 5a 10 5b	C d0 Sail6(50:79), Eu 108.43.121, Dui 30.8 t: 53720, Est Part: 8 79 08 00 45 08 LI 88 25 79 24 59 4	T), . 2.[v	. 1154:74 (40:49:03:51:54:74) Ack: 1, Lon: 9	
0610	66 34 SF 52 49	69 49 96 64 1d c0	a8 2b 79 24 59 .4.	.@.@. d	γ\$Y	
12	wiand: kilve capture	in progress>			Fackets: 3	2 - Displayed: 32 (100.2%) Profile: De

Gambar 3.14. Capturing Data pada Wlan0

13. Langkah pengujian keamanan. Penulis mencoba membuka *website* Unismuh kemudian melakukan *login* pada perangkat *smartphone* korban menggunakan aplikasi Google Chrome terbaru yang terhubung pada jaringan yang sama dengan penyerang.



Gambar 3.15. Proses Login pada Website Unismuh

14. Penulis mencoba membuka *website* Google kemudian melakukan *login* pada perangkat *Smartphone* korban aplikasi Google Chrome terbaru yang terhubung pada jaringan yang sama dengan penyerang.



Gambar 3.16. Google Chrome Menolak Koneksi

15. Penulis mencoba lagi membuka *website* Google kemudian melakukan *login* pada perangkat *Smartphone* korban menggunakan aplikasi *Browser* bawaan *Smartphone* yang terhubung pada jaringan yang sama dengan penyerang.



Gambar 3.17. Browser Memberi Peringatan Keamanan

Karena *Browser* memberi peringatan langsung saja menekan "Lanjutkan" kemudian *login* menggunakan akun Google.

16. Menunggu beberapa saat sampai semua paket data dari *website* Unismuh dan *website* Google ter-*capture*. Selanjutnya menghentikan proses *capturing* pada aplikasi Wireshark dengan cara mengklik "*Stop capturing packet*" pada menu bar seperti pada gambar berikut.

ь. -			
<u>F</u> ile <u>E</u>	dit <u>V</u> iew <u>G</u> o <u>C</u> apt	ure <u>A</u> nalyze <u>S</u> tatistics	Telephony <u>W</u> ireless <u>T</u>
	1 🖉 💿 🗗 🗋	X 🖉 ۹ 🔶 🛪	) (+ +) 🜉
Appl	Stop capturing pack	ets >	
No.	Time	Source	Destination
(	1 0.000000000	192.168.43.121	36.89.54.122
	2 0.000091428	192.168.43.121	36.89.54.122
	3 0.000193176	192.168.43.121	36.89.54.122
	4 0.000324466	36.89.54.122	192.168.43.121
	5 0.000449832	36.89.54.122	192.168.43.121
	6 0.002603385	36.89.54.122	192.168.43.121
	7 0.003625265	192.168.43.121	36.89.54.122
	8 0.003954290	36.89.54.122	192.168.43.121
	Contraction of the second states and the sec		

Gambar 3.18. Menghentikan Proses Capturing

#### **BAB IV**

# HASIL DAN PEMBAHASAN

Analisis perlu dilakukan untuk mengetahui seberapa aman tingkat keamanan yang diterapkan pada *website* Simak Unismuh dan *website* Google Accounts. Seperti yang diketahui tingkat keamanan bukan hanya berasal dari aplikasi *website* yang sudah ada namun keamanan *website* juga dapat dilihat pada saat proses komunikasi data antara *client* dengan *web server* pada jaringan.

Keamanan *website* Simak Universitas Muhammadiyah Makassar masih perlu peningkatan yang terbukti pada hasil percobaan *sniffing* pada aplikasi Wireshark masih ditemukannya paket data berisi informasi penting seperti *username* dan *password* pada saat melakukan *login*, akses *domain name server* (DNS) yang dituju serta informasi lainnya. Disamping itu juga masih banyak masih banyak mahasiswa, dosen, dan staff yang masih awam dengan yang namanya *sniffing* pada jaringan komputer.

#### A. Analisis Hasil Penelitian

Karena dalam penelitian ini menggunakan *hotspot* pribadi yang memiliki kemanan *wifi protected access – pre shared key* (WAP2-PSK), tidak semua orang dapat terhubung pada *hotspot* tersebut. Sehingga penulis tidak menemukan aktifitas yang mengakses akun pada *website* Simak Unismuh. Maka dari itu, penulis melakukan dua skenario yaitu :

1. Skenario Pertama pada Website Simak Unismuh

• Menggunakan akun yang memiliki info sebagai berikut:

- ~ Username : 10582143214.
- ~ *Password* : qwery.
- Login pada pada halaman website Simak Unismuh menggunakan akun diatas.
- Merekam aktifitas yang terjadi menggunakan *software* Wireshark.

Applica	tions 🔻	Places 🔻	🛄 Wiresha	rk <del>v</del>		Sun 03:55		0000 CSL 🗚	N @ 40 B +
8						real fix.pcap	ng		000
<u>File</u>	dit <u>V</u> iew	<u>Go</u> <u>C</u> ap	ture Analyze	Statistics Tel	ephony <u>W</u> ireless <u>T</u>	ools <u>H</u> elp			
	1 2 0		N X C	9. * * .	ə I# #I 🚃 🗐	<u>a</u> a a T			
Apply	y a display	filter <c< td=""><td>1:1-1&gt;</td><td></td><td></td><td></td><td></td><td>E3 •</td><td>Expression +</td></c<>	1:1-1>					E3 •	Expression +
No.	Tin	ne	Source	Destination	Protocol Lengt	th Info			
	10.	9090960	192.158.4	124.81.23.	TCP	74 35338 → 80 [S	YN] Seq=9 Win=14690 Len=9 MSS=1469 S	ACK PERM=1 TSval=189	231 ISec.
	3.8	104/811	192,168 4	192 168 4	1CP	/4 [FCP Retrans] /4 88 - 35338 [5	1155106] 35338 89 [SYN] Seq=9 Win=1 YN_ ACK] Seq=9 Ack=1 Win=28958 Len=9	4600 Len=6 MSS=1466 MSS=1400 SACK PERM=	SAUK PER
	4 0.	1080508	124.81.23	192,168 4.	TGP	74 TCP Recrams	ission] 80 - 35338 [SYN, ACK] Seq-6	Ack-1 Win-28966 Len-	0 MSS=14
	5.0.	1101094	192.188.4	124.81.23	TCP	66 35338 → 80 [/	CK  Seg=1 Ack=1 Win=14720 Len=0 TSva	1=189245 TSepr=26473	5715
	7.0.	1118445	192.168.4	124.61.23	TCP	66 35338 → 80 L	CKl Seg=1 Ack=1 Win=14720 Len=0 TSva	1=189245 TSecr=26473	5715
is.	80.	1119767	192.168.4	124.81.23	TCP	663 TCP Retrans	ission] 35336 - 60 [PSH, ACK] Seq=1	Ack=1 Win=14720 Len=	597 TSV8
	90.	2275643	124.81.23	. 192.168.4.	TCP	66 80 - 35338 [/	ICK] Seq=1 Ack=598 Win=30208 Len=0 T5	val=264735745 TSecr=	189245
6	11 1.	8551924	124.81.23	192,168.4.	1CP	1454 88 - 35338 [A	CK1 Seg=1 Ack=598 Win=36268 Len=1388	ISVal=264/36144 ISe	cr=18924
	12 1.	8551531	124.81.23	192.168.4.	TCP	1454 88 - 35338 [A	CK] Seq=1389 Ack=598 Win=39298 Len=1	388 TSval=264/36144	ISecr=18
	18 1.	8551688	124.81.28	192.168.4	TCP	1454 80 - 35338 [/	CK  Seq=2777 Ack=598 Win=39208 Len=1	388 TSval=264736144	TSecr=18
		8561266	124.81.28	192 168 4	TGP	1454 TCP Out-Of-C	rder] 80 - 35338 [ACK] Sec-1389 Ack	598 Win=36268 Len=13	88 TSval
	16 1.	8562831	124.61.23	192 168 4	TCP	1454 TCP Retrans	ission] 80 - 35338 [ACK] Seq=2777 Ac	k=598 Win=30208 Len=	1366 759
<ul> <li>Fram</li> <li>Ethe</li> <li>Inte</li> <li>Tran</li> <li>Secu</li> </ul>	e 13991 Fract II Fract Pr Smissio Fre Sock	: 284 by , Src: 5 otocol V en Contro ets Laye	rtes on wird GamsungE_5b Version 4, 3 ol Protocol Fr	e (2272 bits :c1:21 (8c:b Src: 192.168 , Src Part:	), 284 bytes cap f:a6:5b:c1:21), .43.121, Dst: 74 56788, Dst Port:	tured (2272 bits) on Dst: LitconTc_10:5b: .125.24.84 443, Scq: 1, Ack: 1	interface 0 73 (2c:d0:5a:10:5b:79) , Len: 218		
6969 6919 6929 6939	20 d9 0 01 Ce 0 18 54 0 00 73	5a 10 5b ae d4 40 dd d4 61 72 a8 60	79 8c bf 96 49 66 bb dc ae 96 61 61	a6 5b e1 21 3c 23 c8 a8 de e1 e5 3d 08 0e 00 03	08 08 45 00 , 2b 79 4a 7d . 0b 05 80 18 . 70 fc de d9 .s	Z.[y[.:E. 			
	real fix						Packets: 14499 · Displaye	ed: 14499 (100.0%)	Profile: Defaul

Gambar 4.1 Hasil Rekaman Paket Data

Pada Gambar 4.1 merupakan tampilan hasil rekaman serangan *packet sniffing* pada *software* Wireshark yang telah merekam seluruh aktifitas yang terjadi pada jaringan.

Untuk melihat paket yang berasal dari *website* Simak Unismuh, maka diharuskan melakukan penyaringan dahulu dari paket yang telah direkam. Sebelum melakukan penyaringan terlebih dahulu, penulis harus mengetahui IP *address* dari *website* Simak Unismuh yang memiliki DNS "simak.unismuh.ac.id" dengan cara membuka terminal kemudian memasukkan perintah "#ping simak.unismuh.ac.id" lalu menekan "Enter" pada keyboard, maka akan muncul IP *address* dari simak.unismuh.ac.id seperti pada gambar berikut.



Gambar 4.2. IP address simak.unismuh.ac.id

Pada Gambar 4.2 dapat diterangkan bahwa angka yang diberi tanda persegi panjang merah merupakan IP *address* dari *website* Simak Unismuh. Setelah mengetahui IP *address* dari simak.unismuh.ac.id yaitu "36.89.54.122", maka selanjutnya melakukan penyaringan paket pada *address bar filter* yang ada dibawah kumpulan *icon* aplikasi Wireshark dengan memasukkan perintah "ip.addr==36.89.54.122" maka akan tampil paket-paket yang memiliki IP *address* tersebut.

Applications - Places - 🚺 Wireshark -	Sun 04:12	1 00.00.05 🖓 🗢 📢 🗗 🗸
	real fix.pcapng	000
File Edit View Go Capture Analyze Statistics Telephony Wireless To	ols Help	
▲ ■ d @ 〒 □ 図 Q + + .J + + 三 目	eea	
Lipseldra-26 80 54 122		Correction 4
R Ipadur-Joursonitze		Contraction of the state of the
No Time Source Destination Protocol Lengt	h lefe	
- 8492 116.15285 192.168.4 36.89.54 TCP 8495 116 15585 192.168.4 36.89.54 TCP	74 33819 - 80 [SYN] Seq=0 Win=14680 Len: 24 [TCP_Retransmission1_32819 - 88 [SYN]	8 MSS=1468 SACK PERM=1 TSval=196057 TSec.
8496 116.22787 192.168.4 36.89.54 TCP	74 33820 → 80 [SYN] Seg=0 Win=14600 Len:	0 MSS=1460 SACK_PERM=1 TSval=196064 TSec.
8497 116.23180 192.168.4. 36.89.54. TCP	74 [TCP Retransmission] 33820 - 80 [SYN	Seq=0 Win=14600 Len=0 MSS=1460 SACK_PER
8498 116.49734 36.89.54 192.168.4 TCP	74 80 - 33819 [SYN, ACK] Seq=0 Ack=1 Wi	=28960 Len=0 MSS=1400 SACK_PERM=1 TSval=
8500 116 57090 36 89 54 192 168 4 TCP	74 EFCP OUL-OF-OFOEFT 80 33818 ESTM /	E28960 Lense MSS=1400 SACK PERM=1 TSVels
8561 116.57162 192.168.4 36.89.54 TCP	66 33819 → 80 [ACK] Seq=1 Ack=1 Win=147;	0 Len=0 TSval=196099 TSecr=59280826
8502 116.57178_ 36.89.54 192.168.4_ TCP	74 [TCP Out-Of-Order] 80 - 33828 [SYN, /	ICK] Seq=0 Ack=1 Win=28960 Len=0 MS5=1400.
8563 116.57192 192.168.4 36.89.54 HTTP	540 GET / HTTP/1.1	
8564 116.57372 192.168.4 36.89.54 TCP	66 33820 - 80 [ACK] Seq=1 Ack=1 Win=1477	20 Len=0 TSVal=196099 TSecr=59280846
8565 116.57571 192.168 4 36.89.54 TCP	548 [TCP PAT answigging] 33819 - 36 [PSH	ACK1 Seget Acket Min=14720 Lenea7A TSya
8587 116.57597 192.168.4 36.89.54 TCP	66 [TCP Dup ACK 8504#1] 33820 - 80 [ACK	Seg=1 Ack=1 Win=14720 Len=0 TSval=19609
8568 116,98797 36.89.54 192.168.4 TCP	66 80 - 33819 [ACK] Seq=1 Ack=475 Win=30	0880 Len=0 TSval=59288930 TSecr=196099
8509 116.90807 36.89.54 192.168.4 HTTP	731 HTTP/1.1 200 OK (text/html)	
Frame 8492: 74 bytes on wire (592 bits). 74 bytes captured	(592 bits) on interface 0	
Ethernet II, Src: SamsungE_5b:e1:21 (8c:bf:a6:5b:e1:21), I	ost: LiteonTe_10:5b:79 (2c:d0:5a:10:5b:79)	
Internet Protocol Version 4, Src: 192.168.43.121, Dst: 36.	89.54.122	
Transmission Control Protocol, Src Port: 33819, Dst Port:	80, Seq: 0, Len: 0	
8000 2c d8 5a 18 5b 79 8c bf a8 5b e1 21 88 88 45 86	Z.[y.,[.]E.	
0010 50 50 10 01 40 60 40 60 05 08 00 88 20 79 24 59 .<	P 5	
8638 39 88 66 fe 86 88 82 84 85 b4 84 82 88 88 86 82 9.	f	
Frame (frame), 74 bytes	Packets: 14499 · Displayed: 2070 (1	4.3%) Dropped: 0 (0.0%) · Load time: 0:0.792 Profile: Default

Gambar 4.3. Hasil Penyaringan Paket Data simak.unismuh.ac.id

Pada Gambar 4.3 merupakan seluruh paket data yang memiliki IP Address 36.89.54.122 yang terdapat pada Source ataupun pada Destination.

Dapat dilihat dari *Source* dan *Destination* yang selalu bertukar tempat. Dari 2070 paket data yang ditampilkan terdapat 2 jenis protokol yang digunakan yaitu protokol *transmission control protocol* (TCP) dan *hypertext transfer protocol* (HTTP). Karena koneksi internet kebanyakan menggunakan protokol TCP maka hasilnya akan banyak paket TCP yang terekam.

Dapat dilihat pula warna dari paket data, terdapat paket yang memiliki warna hijau muda, menunjukkan bahwa paket tersebut menggunakan protokol HTTP dan protokol TCP yang menggunakan port 80. Sedangkan paket yang memiliki warna hitam dengan tulisan merah, menunjukkan bahwa paket tersebut bermasalah dan paket data harus di kirim ulang.

Untuk menganalisis paket data, dapat dilihat pada panel *detail packet* data. Berikut adalah salah satu tampilan *detail packet* data protokol TCP.

Applications 👻 Places 👻 💼 Wireshark 👻	Sun 04:13	🔲 000005 📲 🗟 🕈 📢 🔂 🕶
	real fix.pcapng	000
File Edit View Go Capture Analyze Statistics Telephony Wir	eless <u>T</u> ools <u>H</u> elp	
▲ ■ △ ④ 〒 ○ X ○ へ + +) + +	📜 🖲 e e e 🎹	
ip.addr==36.89.54.122		🖾 🖘 Expression_ +
No Time Source Destination Protocol	Length Jolo	
- 8492 116.15285. 192.168.4. 36.89.54 TCP	74 33819 - 80 [SYN] Seq=0 Win=1	14600 Len=8 MSS=1460 SACK_PERM=1 TSval=196057 TSec.
8496 116.22787., 192.168.4., 36.89.54 TCP	74 33820 → 80 [SYN] Seq=0 Win=1	14600 Len=0 MSS=1460 SACK PERM=1 TSval=196064 TSec.
8497 116.23186 192.168.4. 36.89.54. TCP	74 [TCP Retransmission] 33820	- 88 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PER
8498 116.49734 36.89.54 192.168.4 TCP	74 80 - 33819 [SYN, ACK] Seq=0	Ack=1 Win=28960 Len=8 MSS=1408 SACK_PERM=1 TSval=
8500 116 57090 36 89 54 192 168 4 TCP	74 [1CP 000-01-01-01 00 338. 74 80 → 33820 [SYN, ACK] Sec=8	Ack=1 Win=28960 Len=8 MSS=1400 SACK PERM=1 TSval=
8501 116.57162 192.168.4 36.89.54 TCP	66 33819 - 80 [ACK] Seq=1 Ack=1	1 Win=14728 Len=0 TSval=196099 TSecr=59280826
8502 116.57178_ 36.89.54 192.168.4_ TCP	74 [TCP Out-Of-Order] 80 - 338:	28 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1400_
8563 116.57192 192.168.4 36.89.54 HTTP	540 GET / HTTP/1.1	Use=14720 Lon=0 T5val=106000 TSecr=50200046
8505 116.57571. 192.168.4. 36.89.54 TCP	66 33819 → 80 [ACK] Seg=1 Ack=1	Win=14728 Len=0 TSval=196099 TSecr=59280846
8586 116,57588 192,168,4 36,89,54 TCP	540 [TCP Retransmission] 33819 -	- 80 [PSH, ACK] Seq=1 Ack=1 Win=14720 Len=474 TSva_
8587 116.57597 192.168.4. 36.89.54. TCP	66 [TCP Dup ACK 8584#1] 33820 -	80 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=19609
8566 116.96/97., 36.89.54., 192.168.4., TCP 8569 116 96867 36 89 54 192 168 4 HTTP	00 80 → 33819 [ACK] Seq=1 ACK= 731 HTTP/1 1 200 0K (text/htm]	1/5 Win=30060 Len=0 15Val=59280930 1Secr=196099
	TOT INTER LOO DA (CONCIDENT)	
<ul> <li>Transmission Control Protocol, Src Port: 33819, Ds</li> </ul>	t Port: 80, Seq: 0, Len: 0	
Source Port: 33819		
[Stream index: 54]		
[TCP Segment Len: 0]		
Sequence number: 0 (relative sequence number)		
Acknowledgment number: 0		
Flags: Av082 (SYN)		
0000 2c d2 5a 10 5b 70 9c bf a6 5b a1 21 09 60 45	98. 7.19 1.1.6	
0010 00 3c 1d ef 40 00 46 06 d5 d8 c8 a8 2b 79 24	59 .<	
0020 36 7s 84 1b 00 50 fe 86 e8 36 00 00 00 00 a0	02. 6zP6	
0636 39 08 66 Te 06 68 02 04 05 b4 04 02 08 0a 06	82 9. f	
Frame (frame), 74 bytes	Packets: 14499 · Display	ved: 2070 (14.3%) · Dropped: 0 (0.0%) · Load time: 0:0.792 Profile: Defai

Gambar 4.4. Detail Paket Data TCP simak.unismuh.ac.id

Pada Gambar 4.4 merupakan *detail* dari *packet Transmission Control Protocol* yang diberi tanda persegi panjang merah. Dari Detail paket data tersebut, penulis dapat menganalisis informasi sebagai berikut :

• Source Port: 33819

Menunjukkan port yang digunakan client adalah 33819

• *Destination Port* : http (80)

Menunjukkan port yang digunakan server adalah 80 yaitu http.

• *Flags*: 0x002 (SYN)

Menunjukkan client ingin meminta data dari server.

Karena dalam penelitian ini hanya menganalisis keamanan *website*, maka penulis melakukan penyaringan lagi dengan mengetik perintah "ip.addr==36.89.54.122&&http" maka akan tampil paket-paket yang memiliki protokol HTTP seperti pada gambar berikut.

Applications - Place	es 🔻 🔲 Wireshark 👻		Sun IM:14	🚺 20140CS 🔐 🗢 📢 📴 🗕
			real fix.pcapng	000
<u>File Edit View Go</u>	Capture Analyze Statistics Te	lephony <u>Wireless</u> <u>Tools</u> <u>H</u>	elp	
<b></b>	) 🗋 🖹 🙆 Q + +	ی 📑 🚛 اه ۱۰ د.	e e T	
ip.addr==36.89.54.1	22&&http			🖾 🗔 🔹 Expression 🔸
No. Time	Source Destination	Protocol Length	Info	· · · · · · · · · · · · · · · · · · ·
<ul> <li>B033 116.979</li> <li>B039 116.979</li> <li>B034 116.989</li> <li>B014 116.986</li> <li>B014 117.334</li> <li>B534 117.356</li> <li>B544 117.367</li> <li>B554 117.365</li> <li>B544 117.701</li> <li>B555 417.702</li> <li>B554 117.702</li> <li>B554 117.702</li> <li>B554 117.702</li> <li>B554 117.703</li> <li>B554 117.703</li> <li>B554 117.703</li> <li>B554 117.703</li> <li>B554 117.703</li> <li>B554 117.703</li> <li>B555 117.991</li> <li>B555</li></ul>	192. 197.185 4. 30.89 34 197. 30.88 74. 192.183.4 115. 192.183.4. 30.89.34 115. 192.183.4. 30.89.34 116. 192.183.4. 30.89.54 116. 192.183.4. 30.89.54 116. 192.183.4. 30.89.54 116. 192.183.4. 30.89.54 116. 192.183.4. 30.89.54 107. 30.89.54. 39.218.4 59.5. 30.89.54. 192.183.4 59.5. 30.89.54. 192.183.4 50.8.54. 192.184.4 50.8.54. 192.184.4 50.8.554. 192.184.4 50.8.554. 192.184.4 50.8.554. 192.184.4 50.8.554. 192.184.4 50.8.554. 192.1854.4 50.8.554. 192.1854.4 50.8.554. 192.1854.4 50.8.554. 192	411P         23           H11P         73           H11P         56           HTTP         56           HTTP         56           HTTP         66           HTTP         66           HTTP         66           HTP         62           H11P         52           H11P         52           H11P         52           H11P         52           H11P         52           H11P         54           HTTP         66           HTTP         46           HTTP         66	GET /HT /21.2 HTTP/1.1 200 OK (text/html) GET /ass ts/js/jumery.min.js HTTP/1.1 GET /ass ts/js/jumery.min.js HTTP/1.1 GET /ass ts/js/orghto.js HTTP/1.1 GET /ass ts/js/orghto.js HTTP/1.1 GET /ass ts/js/bootstrap-collapse.js HTTP/1.2 GET /ass ts/js/bootstrap-collapse.js HTTP/1.1 GET /ass ts/js/potestrap-collapse.js HTTP/1.1 HTTP/1.200 WK (application/javascript) HTTP/1.1 200 K (application/javas	.4 L L
Belance Mend Hady           FEldermot II, Sre           Insernet IProtoge           Insernet IProtoge           Insernet II, Sre           Insernet III, Sre           Insernet III, Sre           Insernet III, Sre           Insernet III, Sre           Insernet IIII, Sre           Insernet IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Dytes on wire (4320 bits 5 Samsung-Bb:cl:21 (8c: 01 Version 4, Src: 192.16 Introl Protocol, Src Port: fer Protocol 0 So 78 Sc bf a6 So el 23 49 90 49 56 di 94 cd a8 69 30 fe 86 el 94 cd a8 69 30 fe 86 el 93 cf 57 60 90 61 61 68 94 60 62	<ul> <li>add bytes captured (fractShcc121), Ost: 1</li> <li>d3.121, Dst: 38.89.54</li> <li>33810, Dst Pert: 80, 5</li> <li>33810, Dst Pert: 80, 5</li> <li>48.66, 45.96</li> <li>72, 19</li> <li>73.75</li> <li>74.65</li> <li>75.9</li> <li>74.65</li> <li>75.9</li> <li>75.9</li></ul>	(420 016) 01 01 01 01 01 01 01 01 01 01 01 01 01	
🔘 🗹 Frame (trame),	540 bytes		Packets: 14499 - Displayed: 49 (0.3%) - Dro	pped: 0 (0.0%) + Load time: 0:0.793 Profile: Default

Gambar 4.5. Paket Data simak.unismuh.ac.id dengan Protokol HTTP

Pada Gambar 4.5 merupakan paket data dari *website* Simak Unismuh yang memiliki protokol HTTP. Setelah melakukan penyaringan protokol HTTP, maka sisa paket data yang ditampilkan pada Gambar 4.5 adalah sebanyak 49 paket. Pada menu "Info" terdapat beberapa keterangan seperti GET, HTTP/1.1, dan POST.

Untuk menganalisis paket data tersebut dapat dilakukan dengan cara mengklik kanan paket data pada *listing packet panel* yang ingin dianalisis kemudian pilih *Follow* HTTP *Stream*. Berikut adalah salah satu tampilan detail paket data protokol HTTP yang memiliki info "POST".



Gambar 4.6. Detail Paket Data POST simak.unismuh.ac.id

Gambar 4.6 dapat diterangkan bahwa dari detail paket data protokol HTTP terdapat dua warna teks. Teks yang berwarna merah merupakan HTTP *request* sedangkan teks yang berwarna biru merupakan HTTP *respons*.

Isi dari salah satu paket data yang memiliki info POST berisikan berbagai informasi, diantaranya terdapat informasi sensitif yaitu *username* dan

*password* yang digunakan. Selain itu dalam detail paket data tersebut penulis dapat menganalisis beberapa informasi sebagai berikut :

• POST.

Menunjukkan bahwa *client* melakukan sebuah permintaan dengan memanfaatkan badan pesan untuk mengirim data ke *server web*.

• Host: simak.unismuh.ac.id.

Menunjukkan bahwa client sedang terhubung dengan simak.unismuh.ac.id

• Connection: keep-alive.

Merupakan parameter yang mendefinisikan untuk batas waktu koneksi terputus dan jumlah permintaan maksimum.

- Content-Type: application/x-www-form-urlencoded; charset=UTF-8.
   Menunjukkan bahwa *client* mengirim data melalui *Form Uniform Resource Locator* (URL).
- User-Agent: Mozilla/5.0 (Linux; U; Android 5.1.1; id-id; SM-J200G Build/KTU84P) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30.

Menunjukkan kemungkinan Web browser yang digunakan oleh client.

- Accept-Encoding: gzip,deflate
   Menunjukkan metode kompresi yang diinginkan oleh *client* yaitu gzip atau deflate.
- Accept-Language: id-ID, en-US

Menunjukkan bahasa yang digunakan *web browser* yang dapat di terima server adalah bahasa Indonesia dan bahasa Inggris.

• HTTP/1.1 200 OK.

Menunjukkan permintaan telah berhasil dilakukan.

• Date: Sat, 28 Apr 2018 19:44:35 GMT.

Menunjukkan waktu pada saat server megirim data tersebut.

• Server: Apache

Menunjukkan jenis server yang dipakai yaitu Apache.

Untuk melihat proses komunikasi data pada saat korban mengakses website Simak Unismuh dapat dilakukan dengan cara mengklik "Statistik" pada *menu bar* kemudian pilih "*Flow Graph*" berikut ini adalah tampilannya.

Applications - Places	s 👻 📒 Wireshark 👻	Sun D4:14	1 00 00 CE 🐴 🗟 🖛
		Wireshark - Flow - real fix	000
Time	192.168.43.121	36.89.54.122	Comment
116.571923944	33819 GET / HTTP/1.1	<b>5</b> 0	HTTP: GET / HTTP/1.1
115.908074008	33819 AFTER LAND CALLER	formi, BO	HTTP: HTTP:1.1 200 OK (text@mml)
117 334676254	33819 HTTP/L1 200 OK (tex	fitmi) 80	HTTP: GET Zporta/Z HTTPS_L1
117.356486155	33619 GET /assets/js/jquery.min.js	HTTP/1.1 50	HTTP: GET /assets/js/guery.min/s HTTP/1.1
117.359104270	33820 GET Assets/js/crypto.js H	TTPV1.1 60	HTTP: GET /essetsijs/cryptojs HTTP/L1
117.701404511	33822 GET /assets/js/jquery printElemo	nt/s HTTP/11 - 80	HTTP: GET /sssets/js/guery.printElement.js HTTP/1.1
117.702491430	33624 GE1 /assets/js/bootstrap-dropdo	wnjs-HTTP/12- 80	HTTP: GET /hssetsijs/bootstrap-dropdown.js HTTP/1.1
117.702770265	33821 GET /assets/js/bootstrap-collap	(e); HTTP/1.1 = 80	HTTP: GET /assets/js/footstrap-collapse/s HTTP/1.1
117.705574329	33820 GET /assets@s/many.chained	s VTTP/1.1	HTTP: HTTP:/// 200 OK (application/journality)
117.996959279	33873	= 50 n/jevescript) = 50	HTTP: HTTP://.1.200.OK (spelication/www.srsipt)
118.007818530	30821 HTTP/1.1 200 OK (applicatio	n/jovascript) 50	HTTP: HTTP/1.1 200 OK (application/javascript)
118.083386988	33823 HITP/1.1 200 OK (epplicatio	n/jevascript) 80	HTTP: HTTP:/1.1.200 OK (application/javascript)
118.105856085	33619 HTTP/1.1 200 OK (application	n/jovascript) 60	HTTP: HTTP/1.1 200 OK (spplication/javascript)
118.471870850	92410 GET /assets/css/bootstrap.cs	SHITPALL _ RO	HTTP: GET /assets/css/bootstrap.css HTTP/1.1
4 2 nodes, 49 items			
Show: Displayed packet	s •	Flow type: All Flows -	Addresses: Any -
			Reset
Help			# Close DI Save As

Gambar 4.7. Proses Komunikasi Data simak.unismuh.ac.id

Pada Gambar 4.7 menunjukkan proses komunikasi data antara *client* yang memiliki IP *address* 192.168.43.121 sedangkan server yaitu simak.unismuh.ac.id memiliki IP *address* 36.89.54.122.

- 2. Skenario Kedua pada Website Google Accounts
  - Menggunakan akun yang memiliki info sebagai berikut:

- ~ Username : hasbullah.jj@gmail.com.
- ~ Password : 029962801.
- Login pada pada halaman website Google Accounts menggunakan akun diatas.
- Merekam aktifitas yang terjadi menggunakan *software* Wireshark.

Tampilan hasil rekaman serangan *packet sniffing* pada *software* Wireshark dapat dilihat pada Gambar 4.1 yang telah merekam seluruh aktifitas yang terjadi pada jaringan.

Untuk melihat paket yang berasal dari *website* Google Accounts, maka harus melakukan penyaringan dahulu dari paket yang telah direkam. Sebelum melakukan penyaringan terlebih dahulu, penulis harus mengetahui IP *address* dari *website* Google Accounts yang memiliki DNS "accounts.google.com" dengan cara membuka terminal kemudian memasukkan perintah "#ping accounts.google.com" lalu menekan "Enter" pada keyboard, maka akan muncul IP *address* dari accounts.google.com seperti pada gambar berikut.

[						root@ka	li: ~			0	•	0
File	Edit	View	Search	Terminal	Help							
root	dkal	:~# p	ing aco	counts a	ogle c	om						-
PING	acco	ounts.	google.	.com (74	.125.24	.84) 56(	(84) by	tes of dat	ta.			
64 b	ytes	from	74.125	24.84 ()	74.125.	24.84):	icmp se	eq=1 ttl=4	11 time=202 m	ıs		
64 b	ytes	from	74.125	24.84 (	74.125.	24.84):	icmp se	eq=2 ttl=4	1 time=60.6	ms		
073						L. 168.						ACL
467.4												
4675												ACL

Gambar 4.8. IP address accounts.google.com

Pada Gambar 4.8 dapat diterangkan bahwa angka yang diberi tanda persegi panjang merah merupakan IP *address* dari *website* Google Accounts. Setelah mengetahui IP *address* dari accounts.google.com yaitu "74.125.24.84", maka selanjutnya melakukan penyaringan paket pada *address bar filter* yang ada dibawah kumpulan *icon* aplikasi Wireshark dengan memasukkan perintah "ip.addr==74.125.24.84" maka akan tampil paket-paket yang memiliki IP *address* tersebut.

Appl	lications 👻 🛛 Places 👻 🛄 Wirest	ark 👻	Sun D4:32 •	- ∰ \$> ⇒ 🙀 \$\\0000 [1]
			real fix.pcapng	000
File	Edit View Go Capture Analyza	e Statistics Telephony Wireless T-	ools Help	
		Q + + .J  + +  🚃 🗐		
II ip.	add:==74.125.24.84			🛛 🗔 📲 Expression
No.	Time Source	Destination Protocol Lengt	th Info	-
	12.599 448 42072 199 304 12.5489 448 42072 199 304 12.5489 448 42077 199 304 12.5489 448 42077 199 304 12.5489 448 42075 199 304 199 12.5489 448 42755 199 304 199 12.5489 448 42755 199 304 199 12.5489 448 42763 199 304 199 12.5489 448 42962 74 175 7 12.549 448 49962 74 175 7 12.549 448 49962 74 125 19 12.549 468 09711 192 103 12.549 468 09718 47 125 2 12.549 468 01185, 74 125 2 12.549 468 00774 174 125 2	<ul> <li>4. 74, 125, 24. 10P</li> <li>4. 92, 108, 4. 10P</li> <li>4. 74, 125, 24. 10P</li> <li>4. 10P, 10P</li> <li>4. 102, 10P, 4. 10P</li> <li>4. 10P, 10P, 4. 10P</li> <li>4. 10P, 10P, 4. 10P</li> <li>4. 10P, 12P, 44. 10P</li> <li>4. 10P, 12P, 44. 10P</li> </ul>	/4 55/50 - 443 [SYN] Segne Mi /4 435 - 50/26 [SYN, ACK] Seg 06 55/50 - 443 [ACK] Segn1 AC 74 52222 - 443 [ACK] Segn1 AC 74 52222 - 443 [ACK] Segn1 AC 74 43 - 55/756 [ACK] Segn1 AC 74 443 - 55/756 [ACK] Segn1 AC 74 443 - 55/250 [ACK] Segn1 AC 74 444 - 55/250 [ACK] Segn1 AC 74 444 - 55/250 [ACK] Segn1 AC 75 4 4 4 4 1 [Instit, Segn1 AC 75 4 4 4 1 [Instit, Segn4 AC ] Segn1 AC 75 4 4 4 1 [Instit, Segn4 AC ] Segn1 AC 75 4 4 4 1 [Instit, Segn4 AC ] Segn1 AC 75 4 4 4 1 [Instit, Segn4 AC ] Segn1 AC 75 4 4 4 1 [Instit, Segn4 AC ] Segn1 AC 75 4 4 4 1 [Instit, Segn4 AC ] Segn1 AC 75 4 4 4 [Instit, Segn4 AC ] Segn4 AC ] Segn4 AC ] 75 4 4 4 1 [Instit, Segn4 AC ] Segn4 AC	n=140600 Lence M35541400 SACK PERM=1 ISval=22844/0 ISe. e Abv= Min=28000 Lence M3554400 SACK PERM=1 ISval= k=1 win=16/20 Lence M3554404 M386753/38/2120/ n=20200 Lence M551400 SACK PERM=1 Tokul 020703755 m= 20200 Lence M551400 Lence M5541400 SACK PERM=1 Tokul 020703755 m= 20200 Lence M551400 Lence M5541400 SACK PERM=1 Tokul 020703755 m= 20200 Lence M551400 SACK PERM=1 Tokul 020703757 M564777 Min=35077 Lence M57414000763847 T5647-5793. M564777 Min=35077 Lence M57414000763847 T5647-5793. M56477 Min=35070 Lence M57414000763847 T5647-5793. M56477 Min=35070 Lence M57414000763847 T5647-5793. M5747 Min=35070 Lence M57474 Lence M574740000000000000000000000000000000000
6961 6910 6910 6931	the 32012: 60 bytes on wir hernet II, Src: LiteonTest ternet Protocol Version 4, ausnission Control Protoco 9 60 37 32 83 46 90 48 60 9 10 67 68 61 64 90 48 60 9 10 67 65 61 60 90 61 61	a (522 5155). 45 bytes contin 5:5573 (2crd0;5a:13:55:73), 5rc: 132.166,43.76, Dst: 74. 1, Src Port: 52264, Dst Port: 5a 16 55 79 85 65 45 86 19 76 45 83 20 45 45 86 12 5a 45 69 16 48 99 95	ed (523 bits) on interface 6 Dat: MinomiCo_b1:54:7d (4c:49:c3: 125 24.84 443, Seq: 1056, Ack: 5704, Len: ( 	91:54:7d)
	Frame (trame), 65 bytes		Packets: 14499 - Dis	

Gambar 4.9. Hasil Penyaringan Paket Data accounts.google.com

Pada Gambar 4.9 merupakan seluruh paket data yang memiliki IP Address 74.125.24.84 yang terdapat pada Source ataupun pada Destination.

Dapat dilihat dari *Source* dan *Destination* yang selalu bertukar tempat. Dari 1250 paket data yang ditampilkan terdapat 2 jenis protokol yang digunakan yaitu protokol *transmission control protocol* (TCP) dan *transport layer security* (TLS). Karena koneksi internet kebanyakan menggunakan protokol TCP maka hasilnya akan banyak paket TCP yang terekam.

Dapat dilihat pula warna dari paket data, terdapat paket yang memiliki warna abu-abu muda, menunjukkan bahwa paket tersebut menggunakan protokol TLS dan protokol TCP yang menggunakan port 443. Paket yang memiliki warna abu-abu gelap, menunjukkan bahwa paket tersebut memiliki flag SYN dan FIN ataupun keduanya. Sedangkan paket yang memiliki warna hitam dengan tulisan merah, menunjukkan bahwa paket tersebut bermasalah dan paket data harus di kirim ulang.

Untuk menganalisis paket data, dapat dilihat pada panel *detail packet* data. Berikut adalah salah satu tampilan *detail packet* data protokol TCP.

Applic	ations 👻 🛛 Places 👻	💹 Wireshar	k <del>-</del>		Si	an D4:33 •	- 🖞 (* 🗢 🛪 🖉 0.0000 👔
8					real	fix.pcapng	000
File	Edit View Go Cap	ture Analyze	Statistics Tel	ephony Wire	eless Tools Help		
	1 / @ h	0 8 6	- 2 * * .	J 10 01		T	
lina	dele==74 125 24 84						El Cl - Everession +
[m] aca							
No.	Time 12485-468.42072.	Source . 192.168.4.	Destination 74.125.24.	Protocol TCP	Length Info 74 56758 -	- 443 [SYN]	Seg-0 Win=14800 Len-0 MSS=1486 SACK_PERM-1 TSval=218476 TSe.
	12487 468.42677. 12486 468.42726. 12489 468.42738. 12489 468.42738. 12491 468.49892. 12491 468.49862. 12491 468.52766. 12491 468.51439. 12495 468.51833. 12495 468.51834. 12497 468.51835. 12499 468.51835. 12499 468.51835. 12499 468.51837. 12590 468.5276.	192,168,4, 192,188,4, 192,188,4, 74,125,24, 192,168,4, 192,168,4, 192,168,4, 192,168,4, 192,168,4, 74,125,24, 192,188,4, 74,125,24, 192,188,4, 74,125,24, 192,168,4,	(4,125,24, 74,125,24, 74,125,24, 74,125,24, 192,168,4, 192,168,4, 74,125,24, 192,108,4, (4,125,24, 192,108,4, (4,125,24, 192,168,4, 74,125,24,	. TCP TL Sv1 TCP TCP TCP TLSv1.2 TCP TLSv1.2 TCP TCP TCP TCP TCP TCP TCP TLSv1.2	06 56755 74 5222 284 Client 66 43 + F 74 43 - F 74 43 - F 74 43 - C 66 5222 24 Client 66 43 - C 1454 527 66 52202 1454 5272 66 52202 66 52202 66 52202	- 443 [ACK] 443 [SYN] Hello 16756 [ACK] 12202 [SYN, - 443 [ACK] Hello - 443 [ACK] 16202 [ACK] - 443 [ACK] 16316, Serv. - 443 [ACK]	Seq=1         Ack=1         Win=14/20         Len=0         TSval=2184/9         TSec=3/39/2125/           Seq=0         Min=20200         Len=0         TSval=2184/9         TSec=3/39/2125/           Seq=1         Ack=219         Win=30680         Len=0         TSval=378721264         TSec=218476           AckS         Ack=3400         Len=0         TSval=378721264         TSec=718763         Sec=318/3646           AckS         Ack=1         Win=29312         Len=0         TSval=5620763625         TSec=57930243           Seq=1         Ack=1/1         Win=29312         Len=0         TSval=502970387/         TSec=57930243           Seq=1         Ack=1/1/         Win=32128         Len=0         TSval=52970387/         TSec=57930243           Seq=1/368         Ack=1/7         Win=3520         Len=1368         TSval=57063857         TSec=57930243           Seq=177         Ack=1777         Win=3572         Hin=8772         TSval=1292763827         TSec=579302           FK         Hy AckEnge, Server         Hell Dane         Seq=176365         Sec<17586
- Tra	nemission Contro Baroc Port: 5675 Bestination Port: Stream index: 14 TCP Segment Len: sequence number: ucknowledgment nu (610 Heads -lags: mode2 (SY) no an an 100 80 30 28 02 49 30 57 40 54 61	bl Protocol, 56 : 443 : 9] 6 (relat umber: 0 er Length: 4 N) .9 00 00 06 09 06 bb c0 ca	Src Port: Live sequence 6 bytes (10 10 50 61 41 10 50 7 62 48 10 51 90 89	56756, Dst e number) ) 20 90 44 44 20 79 44 7 90 90 44 44	Part: 443, Seq: 0,	Len: 0	
0030	39 08 46 dd 09 Frame (frame), 74 t	00 02 04 1 bytes	15 54 64 02	96 0á 00 (	93 9.F	Packets:	

Gambar 4.10. Detail Paket Data TCP accounts.google.com

Pada Gambar 4.10 merupakan *detail* dari *packet Transmission Control Protocol* yang diberi tanda persegi panjang merah. Dari detail paket data tersebut, penulis dapat menganalisis informasi sebagai berikut :

• Source Port: 56756

Menunjukkan port yang digunakan client adalah 56756

• Destination Port: 443

Menunjukkan port yang digunakan server adalah 443 yaitu https.

• *Flags*: 0x002 (SYN)

Menunjukkan *client* ingin meminta data dari server.

Karena dalam penelitian ini hanya menganalisis keamanan *website*, maka penulis melakukan penyaringan lagi dengan mengetik perintah "ip.addr==74.125.24.84&&ssl" maka akan tampil paket-paket seperti pada gambar berikut.

Applications 🔻	Places 👻 👩 Wiresh	ark 🕶			Sun D4:33 • 🔟 30:00:02 🗯	} ⇒ 40 B -
					real fix.pcapng	000
File Edit View	Go Capture Analyze	Statistics Te	lephony Wire	less Tools He		
	0 X C	9. * * .	.) I+ +I		२ ९ 🎹	
ip.addr==74.3	25.24.84&&sst				80.	Expression +
No. Tir	ne Source	Destination	Protocol	Length	info	
12489 40	8.42798. 192.168.4		TLSv1	28	Client Hello	
12493 40	8.52768. 192.158.4	74.125.24.	TLSV1.2	24	Client Hello	
12495 40	8.51835 74.125.24	192.168.4.	ILSV1.2	145	Server Hello	
12499 46	8.62274 74.125.24	192.168.4.	TLSv1.2	85	Certificate, Server Key Exchange, Server Hello Done	
12591 46	8.83010 192.168.4		TLSv1.2	15	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
12592 46	8.70802. 74.125.24	., 192.168.4.	TLSv1.2	34	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message	
12503 46	8.73417_ 74.125.24	192.168.4.	TLSV1	103	Server Hello, Certificate, Server Key Exchange, Server Hello Done	
12506 46	8.78773. 192.168.4	74.125.24.	TLSV1	26	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
12508 46	8.8382274.125.24	192.168.4.	TLSV1	31	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message	
12518 40	8.88403. 192.158.4	74.125.24.	ILSV1	28	Client Hello	
12524 40	8.98265. 192.168.4	/4.125.24.	ILSV1.2	24	Client Hello	
12526 46	9.96647 74.125.24	192.168.4.	TLSV1.2	145	Server Hello	
12030 40	9.00/13 74.120.24	192.105.4.	TLSVI.2	80	Gertificate, server key Exchange, server Heild bone	
12032 40	9.00408. 192.108.4		TLSV1.2	11	utient key exchange, change uipner spec, Encrypted Handshake Message	
12033 40	9.1070474.125.24	192.105.4.	TLSV1.2	34	New Session Floket, Change Cipner Spec, Encrypted Manushake Message	
12534 40	9.10700. 74.125.24	192.105.4.	TLSVI	103	server Hello, Certificate, Server Key Exchange, Server Hello Done	
				WARDING WORKSHIP IN		
Frame 12485	1: 284 bytes on wir	e (2272 Dili	1), 284 Dyte	es captured	272 HILS) ON INTERFACE 0	
ethernet II	, are: samsunge_au	icitzi (ouit	in actobici.	(ZI), DSLI L	conte_ta:so:/s (zeroa:se:te:so:/s)	
Incernet Pr	otocol version 4,	SFC: 192.108	43.121, D	st: 74.125.2		
Transmissio	on Control Protocol	, SFC Port:	56755, DSt	Port: 443,	2q: 1, ACK: 1, LCN: 218	
> Secure Socx	ets Layer					
6969 2c d9	5a 10 5b 79 8c bf	ati 5b e1 21	88 68 45 6	6 . Z. Ly	· Latas E.	
6919 01 Ce	70 04 45 50 45 50	02 13 08 48	2b 79 4a 7	0 ( .8.0.	- + y 3 )	
	20 01 10 00 10 00			Let		
3929 18 54	dd b4 61 bb c5 ea.	7d 65 86 1F		B	)e	
1020 18 54 1030 00 73	dd b4 61 bb c5 ea 22 85 00 90 91 01	/d 65 00 1f	f2 de 80 1 55 66 de d	ι ε	)e	

Gambar 4.11. Paket Data accounts.google.com dengan Protokol TLS

Pada Gambar 4.11 merupakan paket data dari *website* Google Accounts yang memiliki protokol TLS. Pada menu Info terdapat beberapa keterangan seperti *Clint Hello*, *Server Hello*, *Certificate*, *Server Key Exchange*, *Encrypted Handshake Message*, *Client Key Exchange*, *Change Cipher Spec*, *New Session Ticket*, dan *Application Data*.

Untuk menganalisisnya dapat dilakukan dengan cara mengklik kanan pada paket data yang ingin dianalisis kemudian pilih *Follow* SSL *Stream*. Berikut adalah salah satu tampilan *detail packet* data protokol TLS yang memiliki info *Application Data*.



Gambar 4.12. Detail Paket Data Application Data accounts.google.com

Pada Gambar 4.12 merupakan tampilan dari *Follow* SSL *Stream* dan *Follow* TCP *Stream* dari data yang dipilih. Dari detail paket data protokol TLS pada gambar tersebut, tidak ditemukan infomasi apapun. Maka dari itu, penulis melalukan analisis pada paket data yang sama dengan cara mengklik kanan pada paket data yang ingin dianalisis kemudian pilih *Follow* TCP *Stream*. Berdasarkan panel *Follow* TCP *Stream*, penulis tidak dapat menganalisis informasi dengan mudah. Hal ini dikarenakan data yang dikirim telah dienskripsi.

Untuk melihat proses komunikasi data pada saat korban mengakses *website* Google Accounts dapat dilakukan dengan cara mengklik "Statistik" pada menu bar kemudian pilih "*Flow Graph*" berikut ini adalah tampilannya.



Gambar 4.13. Proses Komunikasi Data accounts.google.com

Gambar 4.13 menunjukkan proses komunikasi data antara *client* yang memiliki IP *address* 192.168.43.121 sedangkan server yaitu accounts.google.com memiliki IP *address* 74.125.24.84.

# **B.** Pembahasan

Hasil dengan dilakukannya analisis uji coba dalam penelitian ini menunjukkan bahwa *website* Simak Unismuh rentan terhadap pencurian data dengan menggunakan metode serangan *sniffing* pada jaringan nirkabel. Hal ini terjadi karena pada website Unismuh masih menggunakan protokol HTTP sedangkan *website* Google Accounts menggunakan protokol TLS. Perbedaanya yaitu terletak pada cara kerjanya.

Pada saat target mengakses *website* Simak Unismuh menggunakan browser, kemudian browser meminta data pada server, server langsung mengirim data yang di minta dalam bentuk teks biasa melalui TCP tanpa adanya perlindungan lebih. Sehingga pada saat melakukan proses *sniffing*, seluruh data yang melewati komputer penyerang akan ter-*capture* pada aplikasi wireshark dan data tersebut dapat dibaca langsung oleh penyerang seperti yang terlihat pada Gambar 4.6.

Berdasarkan Gambar 4.7 secara sederhana proses komunikasi data *website* Simak Unismuh digambarkan sebagai brikut.



Gambar 4.14. Proses Komunikasi Data Website Simak Unismuh

Gambar 4.14 secara sederhana merupakan proses komunikasi antara *client* dengan server *website* Simak Unismuh. Dapat dilihat bahwa pada saat *client* melakukan sebuah permintaan untuk mangambil data dari *web sever* terdapat 2 opsi yaitu menggunakan metode GET atau menggunakan metode POST.

Pada saat *client* melakukan sebuah permintaan dengan menentukan paramater di bagian URL dari permintaan maka metode permintaan HTTP tersebut berisikan opsi GET, contohnya yaitu URL yang terdapat pada halaman *website*. Sedangkan jika *client* melakukan sebuah permintaan dengan memanfaatkan badan pesan untuk mengirim data ke *server web* maka metode permintaan HTTP tersebut berisikan opsi POST, contohnya yaitu *form* pengisian *username* dan *password* pada halaman *website*. Setelah itu server mengirimkan HTTP *response* ke *client* yang berisikan data yang diminta dalam bentuk *plaintext*.

Berbeda halnya dengan *website* Google Accounts. Pada saat target mengakses *website* Google pada *browser*, kemudian *browser* (*client*) meminta data pada server, server tidak langsung mengirimkan data yang diminta. Tetapi *client* dan server melakukan kontak terlebih dahulu untuk membuktikan identitasnya kemudian melakukan negosiasi kode rahasia sebelum melakukan pertukaran data. Sehingga pada saat melakukan proses *sniffing*, data yang melewati komputer penyerang tidak dapat dibaca langsung pada aplikasi Wireshark seperti yang terlihat pada Gambar 4.12.

Berdasarkan Gambar 4.13 secara sederhana proses komunikasi data *website* Google digambarkan sebagai berikut.

Client IP 192.168.43.121 Server IP 172.217.24.4



Gambar 4.15. Proses Komunikasi Data Website Google Accounts

Gambar 4.15 merupakan proses komunikasi secara sederhana antara *client* dengan server *website* Google Accounts. Dapat dilihat bahwa *client* mengirimkan pesan "*Client Hello*" ke server. Setelah itu server merespon dengan mengirim pesan "*Server hello*" ke *client* bersama dengan *public key* server untuk melakukan pertukaran *public key* dengan *client*. Selain itu server juga mengirimkan

sertifikatnya ke *client* untuk di otentikasi, kemudian server mengirim pesan "Server *hello done*". Jika sertifikat ditandatangani oleh salah satu CA (*certification authority*) di dalam daftar CA yang dipercaya telah terdaftar di dalam *web browser*, maka *client* dapat menverifikasi *public key* server. Selanjutnya *client* mengirimkan pemberitahuan "*Change Cipher Spec*" ke server untuk menunjukkan bahwa *client* akan memulai menggunakan *public key* untuk mengenkripsi pesan. Kemudian server memulai sesi baru dengan mengirimkan pemberitahuan "*Change Cipher Spec*" ke server akan memulai menggunakan tiket sesi yang mencakup semua pesan yang dinegosiasikan sebelumnya yang dienkripsi dengan *secret key* yang hanya diketahui server. Setelah itu *client* dan server tetapkan.

Apabila pengiriman data telah selesai, dan *client* ingin meminta data lagi pada server maka *client* mengirimkan pesan "*Client* hello" menggunakan ID sesi dari sesi sebelumnya. Kemudian server memeriksa *session cache* untuk mencocokkan ID sesi tersebut. Jika ditemukan kecocokan, server dapat melanjutkan sesi dan mengirimkan pesan "Server hello", lalu *client* dan server bertukar pesan "*Change Cipher Spec*". *Client* dan server dapat mengirim data aplikasi melalui saluran aman yang telah *client* dan server tetapkan.

## C. Solusi untuk Mencegah Serangan Packet Sniffing

Setelah melakukan penelitian, penulis telah menyiapkan beberapa rekomendasi solusi untuk meningkatkan keamanan terhadap serangan seperti yang dilakukan penulis.

- 1. Pengguna Website.
  - a. Menggunakan keamanan enkripsi WPA2-PSK pada *hotspot wifi*. Dengan menggunakan sistem keamanan pada *wifi* maka hanya orang-orang tertentu saja yang dapat terhubung ke jaringan. Sehingga serangan *sniffing* tidak bisa dilakukan oleh orang lain yang tidak terhubung pada jaringan tersebut.
  - b. Memperbaharui *browser* ke versi yang terkini. Keamanan pada *browser* versi lama beresiko terhadap berbagai serangan, karena kemungkinan celah keamanan *browser* versi lama telah diketahui dan dapat digunakan untuk mencuri informasi sensitif. Menggunakan *browser* versi terkini menjamin keamanan pada saat terhubung dengan internet, karena pada *browser* versi terkini menyimpan daftar informasi sertifikat *secure socket layer* (SSL) dari berbagai situs web dalam upaya mencegah serangan *man in the middle* (MITM).
- 2. Developer Website.
  - a. Menggunakan sertifikat SSL pada *website* Simak Unismuh. Dengan menggunakan sertifikat SSL informasi sensitif akan terjaga selama dalam proses pengiriman melalui internet dengan cara dienkripsi, sehingga hanya penerima pesan yang dapat memahami dari hasil enkripsi tersebut. Hal ini penting karena informasi yang dikirim di internet membutuhkan proses perjalanan dari komputer ke komputer sampai mencapai server tujuan. Komputer lain yang ada diantara komputer *user* dan server dapat melihat informasi sensitif seperti *username* dan *password* bila tidak dienkripsi dengan sertifikat SSL.

#### BAB V

#### PENUTUP

# A. Kesimpulan

Dari hasil penelitian yang telah dilakukan maka dapat ditarik simpulannya, yaitu:

- Tingkat keamanan website Simak Unismuh masih perlu ditingkatkan. Hal ini dibuktikan dengan penyerangan packet sniffing yang dapat merekam dan menampilkan informasi sensitif seperti username dan password dengan menggunakan aplikasi wireshark.
- 2. Karena *website* Simak Unismuh belum menggunakan sertifikat SSL, maka sangat rentang terhadap serangan MITM (*man in the middle*) meski *browser* yang digunakan merupakan versi terbaru.
- 3. Untuk mencegah atau menghindari serangan *packet sniffing* dapat dilakukan dengan cara sebagai berikut :
  - a. Menggunakan keamanan enkripsi WPA2-PSK pada hotspot wifi.
  - b. Memperbaharui *browser* ke versi yang terkini. Keamanan pada *browser* versi lama beresiko karena kemungkinan celah keamanan *browser* versi lama telah diketahui dan dapat digunakan untuk mencuri informasi sensitif.
  - c. Menggunakan sertifikat SSL pada *website* Simak Unismuh. Hal ini dilakukan untuk menjaga informasi sensitif akan selama dalam proses pengiriman melalui internet dengan cara dienkripsi.

# **B.** Saran

Berdasarkan uraian dari kesimpulan, maka kekurangan di atas dapat menjadi pelajaran serta referensi untuk ke depannya. Saran – saran yang dapat dipertimbangkan untuk ke depan antara lain :

- 1. Jika *wifi* sudah menggunakan keamanan enkripsi WPA2-PSK, Sebaiknya tidak memberitahukan *password wifi* ke sembarang orang.
- 2. Sebaiknya dilakukan penggantian *password wifi* secara berkala untuk menghindari terjadinya penyusupan oleh pihak yang tidak bertanggung jawab.
- 3. Tidak mengabaikan pembaritahuan *update* jika terdapat pemberitahuan dari *browser*.
- 4. Diperlukannya sertifikat SSL sebagai keamanan bagi *website* untuk meminimalisir sebelum terjadinya serangan *man in the middle*.

#### DAFTAR PUSTAKA

- Adriant, M.F., & Mardianto, I. (2015). Seminar Nasional Cendekiawan. Implementasi Wireshark untuk Penyadapan (Sniffing) Paket Data Jaringan, 2, 224-228. Retrieved from <u>http://www.trijurnal.lemlit.trisakti.</u> ac.id/index.php/semnas/article/view/139.
- Basri. (2015). Jurnal Ilmu Komupter. Pendekatan Kriptografi Hybrid pada Keamanan Dokumen Elektronik dan HypertextTransfer Protocol Secure (HTTPS) (Analisis Potensi Implementasi Pada Sistem Keamanan), 1(2). Retrieved from <u>https://ejournal.fikom-unasman.ac.id/index.php/jikom/</u> <u>article/view/34</u>.
- Dewi, R., Rimra, I.L., & Vitria, R. (2012). Poli Rekayasa. Analisis Komunikasi Data Pada Aplikasi Percakapan Suara Menggunakan Perangkat Lunak Wireshark, 8(1), 32-41. Retrieved from <u>http://repo.polinpdg.ac.id/273/</u>.
- Hamid. (2017). Teknoin. Analisis Keamanan Aplikasi Email Bawaan Android dan Gmail Pada Jaringan Nirkabel, 23(2), 125-136. Retrieved from http://jurnal.uii.ac.id/jurnal-teknoin/article/view/8923.
- Khairina, D.M. (2011). Jurnal Informatika Mulawarman. *Analisis Keamanan Sistem Login*. 6(2), 64-67. Retrieved from <u>https://jurnalinforman.wordpress.com/2013/03/30/analisis-keamanan-sistem-login/</u>.
- Nazwita, & Ramadhani. S. (2017). Seminar Nasional Teknologi Informasi, Komunikasi dan Industri (SNTIKI). Analisis Sistem Keamanan Web Server dan Database Server Menggunakan Suricata, 9, 308-317. Retrieved from <u>http://ejournal.uin-suska.ac.id/index.php/SNTIKI/article/view/3368</u>.
- Pranata, H., Abdillah, L.A., & Ependi, U. (2015). Student Colloquium Sistem Informasi & Teknik Informatika (SC-SITI). Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan, 1, 1-6. Retrieved from <u>http://eprints.binadarma.ac.id/2404/</u>.

Rerung, R.R. (2018). Program Web Dasar. Deepublish. Yogyakarta.

Rosnelly, R., & Pulungan, R. (2011). Konferensi Nasional Sistem Informasi. Membandingkan Analisa Trafik Data pada Jaringan Komputer antara Wireshark dan NMAP, 1, 936-947. Retrieved from <u>http://pulungan.staff.ugm.ac.id/pubs/RP-KNSI-11.pdf</u>.

- Singh, A. (2013). *Instant Wireshark Starter*, Packt Publishing Ltd, Birmingham B3 2PB.
- Supriyanto, A. (2006). Jurnal Teknologi Informasi Dinamik. Analisis Kelemahan Keamanan pada Jaringan Wireless, 11(1), 38-46. Retrieved from <a href="http://www.unisbank.ac.id/ojs/index.php/fti1/article/view/33">http://www.unisbank.ac.id/ojs/index.php/fti1/article/view/33</a>.
- Wikipedia. (2018, Januari 5). Ensiklopedia Bebas. *Transport Layer Security* ,Diakses pada 11:50, Januari 5, 2018, dari <u>https://id.wikipedia.org/w/index.php?title=Transport\_Layer\_Security&oldi</u> <u>d=13502518</u>
- Wikipedia. (2018, Februari 15). Ensiklopedia Bebas. *Situs Web*, Diakses pada 15:38, Februari 15, 2018, dari <u>https://id.wikipedia.org/w/index.php?</u> <u>title=Situs\_web&oldid=13705588</u>.
- Wireshark. (2018). Wireshark Go Deep. Wireshark User's Guide, Diakses pada 15:45, Februari 15, 2018, dari https://www.wireshark.org/docs/wsug\_html/\_
- Yani, A. (2009).Panduan Membangun Jaringan Komputer (ed. Revisi; Utility Jaringan), Kawan Pustaka, Jakarta.
- Zam, E. (2016). Buku Sakti Wireless Hacking, PT Elex Media Komputindo, Jakarta.

# LAMPIRAN

# LAMPIRAN 1

#### Tampilan Halaman Website



Gambar L1-1. Halaman Website Simak Unismuh


Gambar L1-2. Halaman Website Google Accounts

### LAMPIRAN 2

## Dialog Box sebagai Data Tambahan untuk Menganalisis Paket Data pada

# Aplikasi Wireshark

lame	Filter
Bad TCP	tcp.analysis.flags && Itcp.analysis.window_update
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	stp.type == 0x80
OSPF State Change	ospf.msg != 1
CMP errors	icmp.type eq 3    icmp.type eq 4    icmp.type eq 5    icmp.type eq 11    icmpv6.type eq 1    ic
ARP	arp
ICMP	icmp    icmpv6
TCP RST	tcp.flags.reset eq 1
SCTP ABORT	sctp.chunktype eq ABORT
TTL low ar unexpected	(!ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && lospf)    (ip.dst == 224.0.0.0/24 && ip.dst
Checksum Errors	eth.fcs.status=="Bad"    ip.checksum.status=="Bad"    tcp.checksum.status=="Bad"    udp.che
SMB	smb    nbss    nbns    nbipx    ipxsap    netbios
I HTTP	http    tcp.port == 80    http2
/ IPX	ipx    spx
DCERPC	dcerpc
Routing	hsrp    eigrp    ospf    bgp    cdp    vrrp    carp    gvrp    igmp    ismp
TOP SYN/FIN	tcp.fiags & 0x02    tcp.fiags.fin == 1
TOP	tcp
UDP	udp
7 Broadcast	eth[0] & 1
1	

## Gambar L2-1. *Coloring Rules* Wireshark

	Wireshark · Display Filters	C
Name	Filter	
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00	
Ethernet type 0x0806 (ARP)	eth.type == 0x0806	
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff	
No ARP	not arp	
IPv4 only	ip	
IPv4 address 192.0.2.1	lp.addr == 192.0.2.1	
IPv4 address isn't 192.0.2.1 (don't use != for this!)	!(ip.addr == 192.0.2.1)	
IPv6 only	ipv6	
IPv6 address 2001 db8::1	ipv5.addr == 2001:db8::1	
IPX only	ipx	
TCP only	tcp	
UDP only	udp	
Non-DNS	I(udp.port == 53    tcp.port == 53)	
TCP or UDP port is 80 (HTTP)	tcp.port == 80 [] udp.port == 80	
HTTP	http	
No ARP and no DNS	not arp and !(udp.port == 53)	
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp.port in {80 25}	
+ - 0		© Cancel ✓ OK

Gambar L2-2. Display Filter Wireshark

### **LAMPIRAN 3**

#### **Surat Penelitian**

## UNIVERSITAS MUHAMMADIYAH MAKASSAR FAKULTAS TEKNIK



والله الحقار الحقاء ->

Nomor : 216/05/C.4-VI/IV/39/2018 Lamp.

Hal

Makassar, <u>10 Sya'ban 1439 H</u> 26 April 2018 M Permohonan Data dalam Penyelesaian Tugas Akhir

Kepada yang Terhormat, Kasubit IT Universitas Muhammadiyah Makassar Di-Tempat

Assalamu 'Alaikum Warahmatullahi Wabarakatuh

Dengan Rahmat Allah SWT, Sehubungan dengan rencana penelitian tugas akhir, mahasiswa Universitas Muhammadiyah Makassar tersebut di bawah ini :

Hasbullah Jamaluddin (105 82 1404 141432 14) Nama Nurul Fitriani Suaeb (105 82 1405 14) Jurusan **Teknik Elektro** Judul TugasAkhir : Analisis Keamanan Website terhadap Sniffing Process Pada Jaringan Nirkabel Menggunakan Aplikasi Wireshark.

Untuk Keperluan diatas, kiranya dapat diberikan izin untuk Pengambilan Data" Topologi Jaringan" Pengambilan data tersebut selama 1 Minggu guna keperluan penelitian. Data tersebut diperlukan dalam rangka penyelesaian Tugas Akhir pada Fakultas Teknik Jurusan Teknik Elektro Universitas Muhammadiyah Makassar.

Demikian permohonan kami atas perhatian dan kerjasama Bapak di haturkan banyak terima kasih.

	authtras 7	Hummean?
		Alm. or heref
		Hamzah Al Imran, S.T., M.
	Deki	055 500
Temh	usan: Kepada Yang Terhormat.	
1	Rektor Unismuh Makassar	
2	Ketua Jurusan elektro	
3	Arsip : C:/Dokumen/tata usaha/mahasiswa/pengantar	

Gambar L3-1. Surat Permohonan Penelitian

### LAMPIRAN 4

### **Dokumentasi Penelitian**



Gambar L4-1. Melakukan Login pada Website Simak Unismuh dan Google

Accounts



Gambar L4-2. Menganalisis Paket Data yang Tertangkap pada Aplikasi Wireshark