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

HASBULLAH JAMALUDDIN
105 82 1432 14

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

بسم الله الرحمن الرحيم

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

بسم الله الرحمن الرحيم

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.

Makassar, 15 Ramadhan 1439 H
31 Mei 2018 M

Panitia Ujian :

1. Pengawas Umum
   a. Rektor Universitas Muhammadiyah Makassar
      Dr. H. Abd. Rahman Rahim, SE.,MM : .....
   b. Dekan Fakultas Teknik Universitas Hasanuddin
      Dr. Ir. H. Muhammad Arsyad Thaha, M.T : .....
2. Penguji
   a. Ketua : Andi Faharuddin, ST.,MT : .....
   b. Sekretaris : Adriani, 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	Pembimbing II
Dr. H. Zulfajri Basri Hasanuddin, M.Eng	**Rahmania, ST.,MT**

Dekan

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

KATA PENGANTAR

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.
2. Bapak Ir. Hamzah Al Imran, S.T., M.T. selaku Dekan Fakultas Teknik Universitas Muhammadiyah Makassar.

3. Bapak Dr. Umar Katu, S.T., M.T. selaku ketua Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Makassar.
4. 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.
5. 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[1], Nurul Fitriani Suaeb[2]

[1,2]Jurusan Teknik Elektro Fakultas Teknik Universitas Muhammadiyah Makassar

E-Mail: [1]hasbuloke@gmail.com, [2]suaebnurul@gmail.com

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[1], Nurul Fitriani Suaeb[2]

[1,2]Department of Electrical Engineering, Faculty of Engineering, Muhammadiyah University of Makassar

E-Mail: [1]hasbuloke@gmail.com, [2]suaebnurul@gmail.com

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

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

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
TCP	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
CA	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.
2. 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 :

1. 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.

2. 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 :

1. 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).

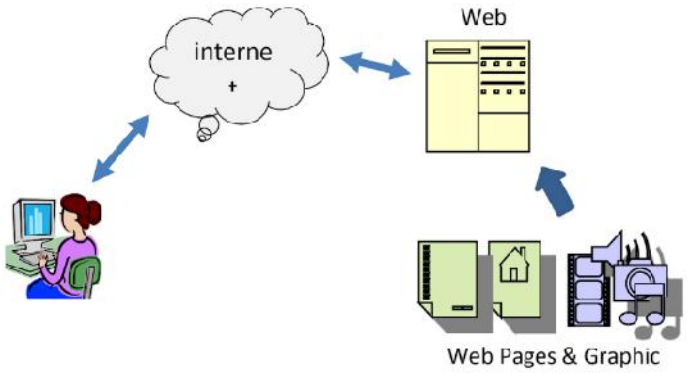
1. Web Server

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).

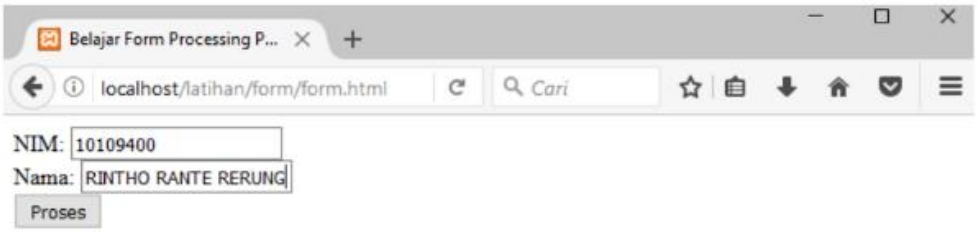
1. *Atribut Action*

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*

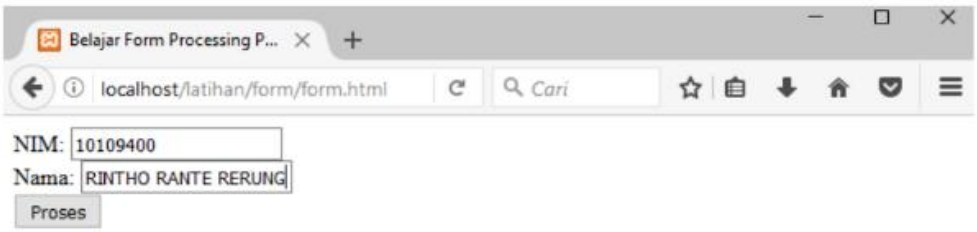
Atribut method adalah atribut yang akan menentukan bagaimana cara *form* dikirim di dalam halaman proses.php. Nilai dari atribut *method* hanya bias diisi dengan satu dari dua pilihan, yakni GET atau POST. *Method* GET akan membuat nilai dari *form* yang akan dikirim melalui alamat URL *website*. Namun 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)

Gambar 2.3. Hasil Proses *Form* Menggunakan *Method* 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 mcnggunakan TCP, diwajibkan membentuk hubungan (*handshake*) terlebih dahulu. Kemudian, dalam proses pertukaran data, TCP mengimplementasikan proses deteksi kesalahan paket dan re-transmisi dan semua proses ternasuk pengiriman paket data ke tujuan secara berurutan (Yani, 2009).

2. *Application Layer*

Di dalam model OSl, 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

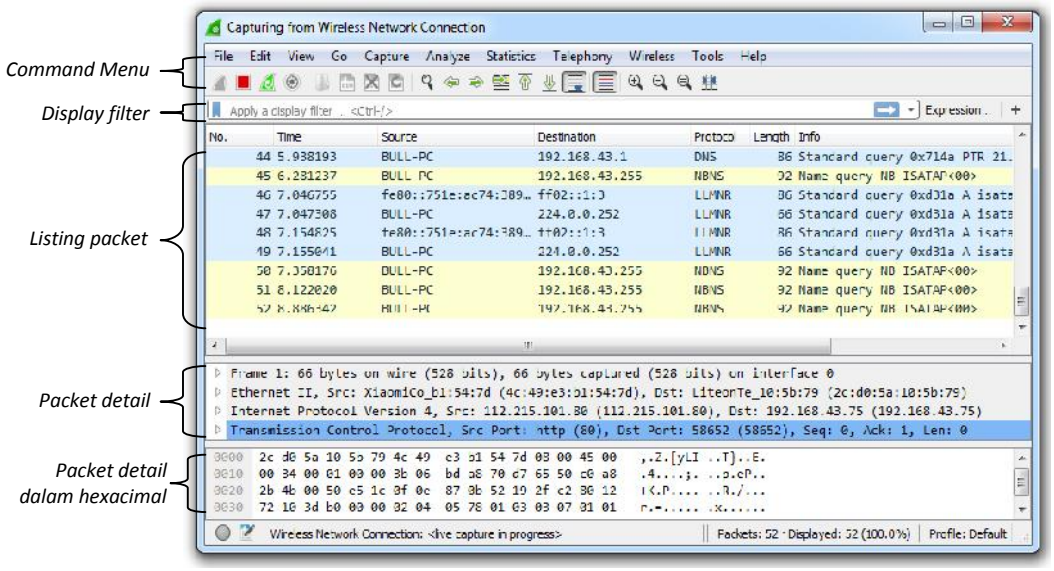
Wireshark adalah alat penganalisis paket jaringan *open source* yang menangkap paket data yang melewati jaringan dan menyajikannya dalam bentuk yang dapat dimengerti. Wireshark dapat dianggap sebagai pisau tentara Swiss karena dapat digunakan dalam situasi yang berbeda seperti masalah jaringan, operasi 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.

Tabel 2.1. Persyaratan Sistem Aplikasi Wireshark.

Feature	*Description*
OS	Windows *any version*, Apple macOS, Linux, Solaris, FreeBSD, NetBSD, *any other*.
Processor	*Any modern* 64-bit AMD64/x86-64 or 32-bit x86 *processor*.
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, *and other*.

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).

Tabel 2.2. Informasi Yang Dapat Diambil Dari Serangan *Sniffing*.

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*

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 materi-materi 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.

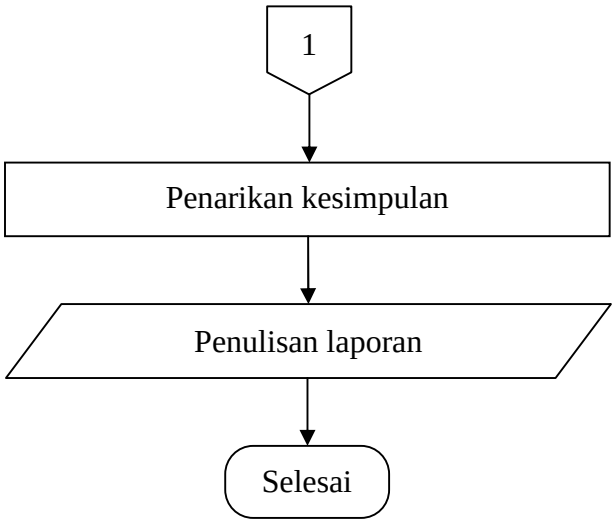
C. Teknik Analisis Data

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.
3. 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*).

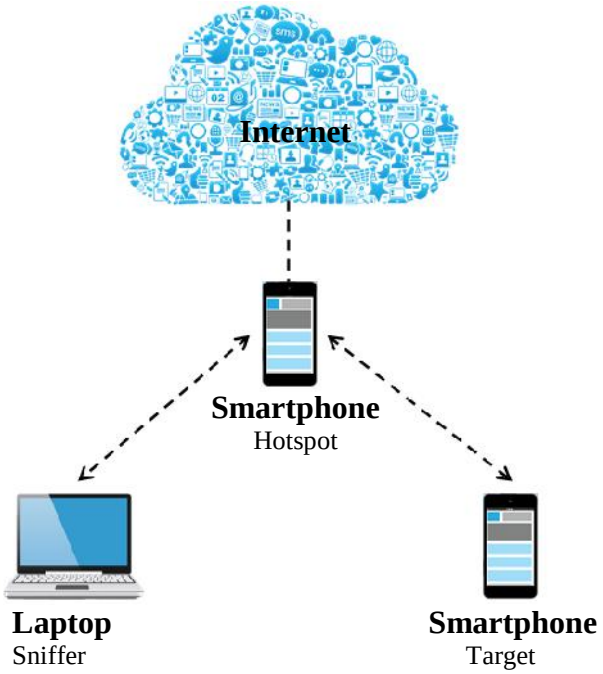
F. Tahapan-tahapan Konfigurasi Software

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*).

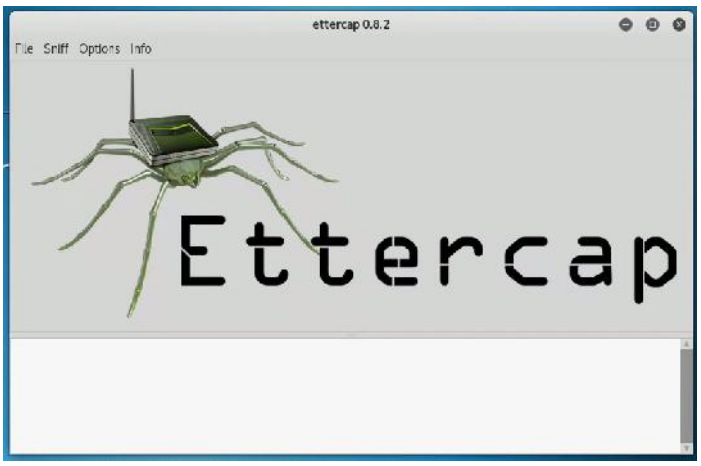
Pada analisa ini terlibat komponen perangkat yang saling berhubungan, yaitu: jaringan internet, wifi *hotspot* yang bersal dari *smartphone*, laptop penyerang dan *smartphone* target. Untuk lebih jelasnya dapat dilihat pada gambar berikut.



Gambar 3.2. Topologi Jaringan Penelitian

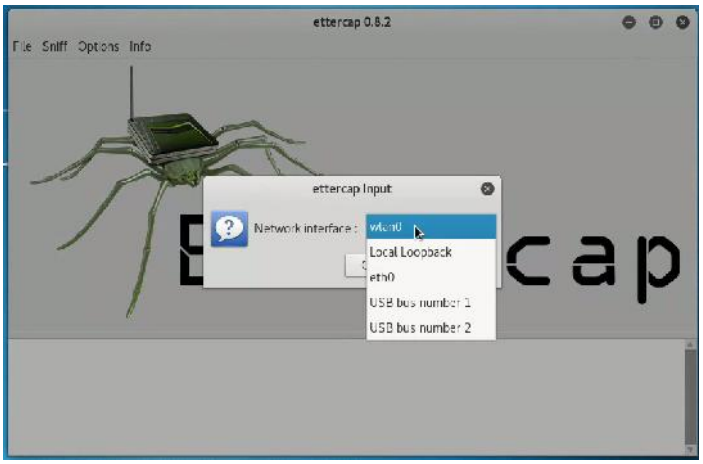
Setelah mengetahui skema yang ditunjukkan pada Gambar 3.9, maka langkah selanjutnya yaitu pengujian keamanan bertujuan untuk memperoleh kesadaran akan permasalahan keamanan pada *website* yang dikunjungi.

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.



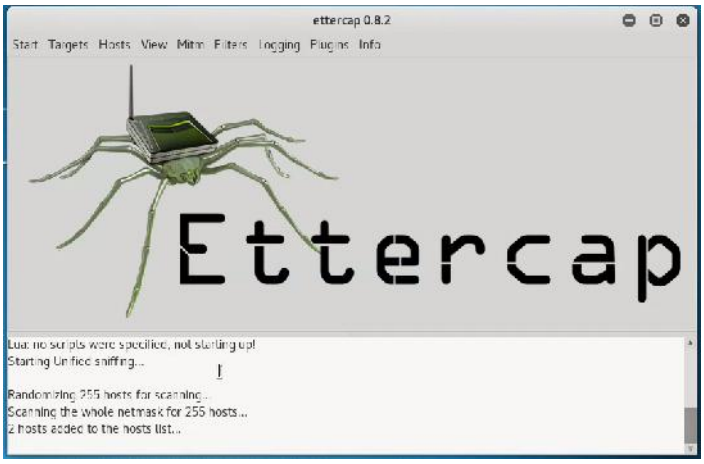
Gambar 3.3. Tampilan Awal Aplikasi Ettercap

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

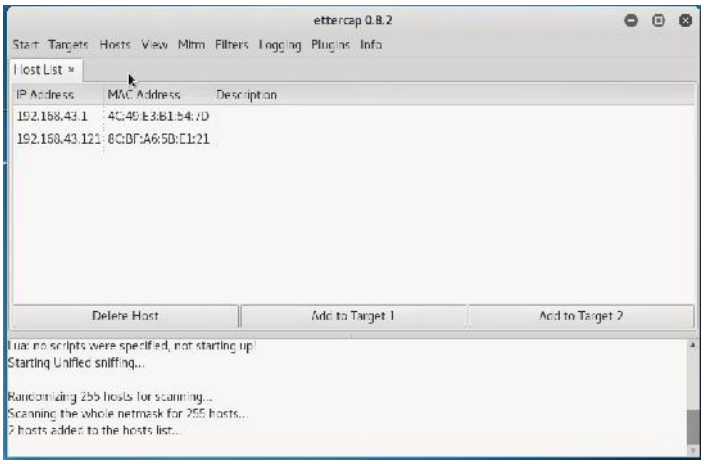
4. Meng-*scan host* yang ada di dalam jaringan dengan cara mengklik menu "*Hosts*" kemudian pilih "*Scan for hosts*" lalu tunggu sampai proses *scanning* selesai. Setelah proses *scanning* selesai maka akan terlihat jumlah *host* yang terhubung pada jaringan yang sama dengan penyerang.



Gambar 3.5. Tampilan Setelah Proses *Scanning*

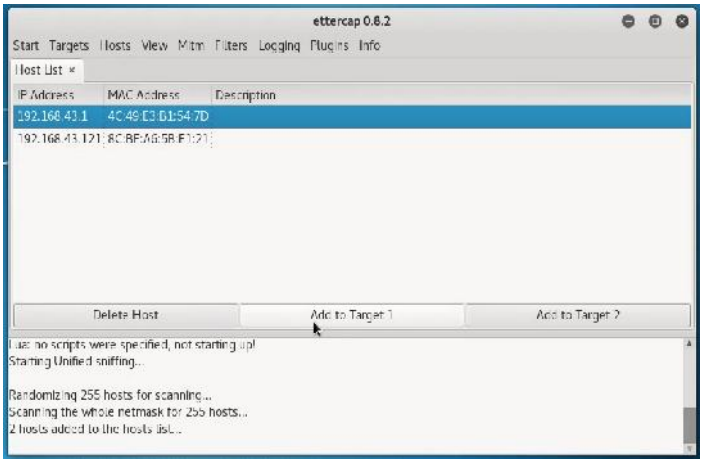
Pada Gambar 3.5 terdapat 2 *hosts* yang terhubung pada jaringan yang sama.

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.



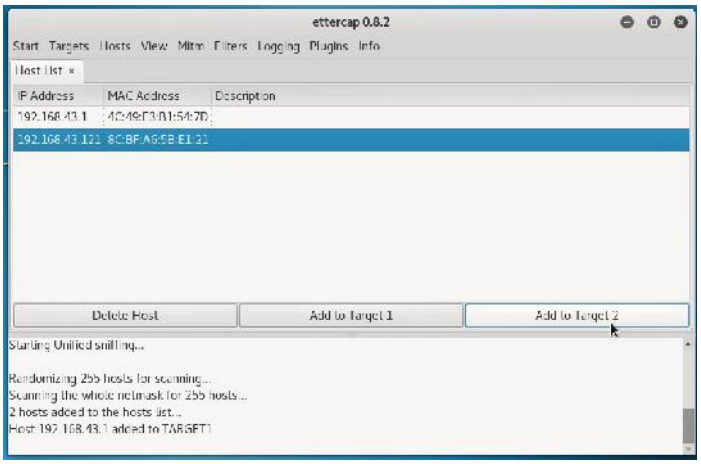
Gambar 3.6. Tampilan Daftar *Hosts*

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*.



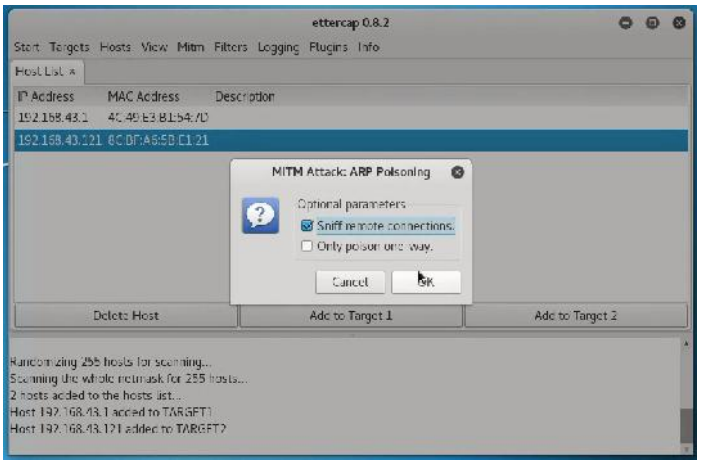
Gambar 3.7. Menambahkan IP Gateway sebagai Target 1

7. 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.



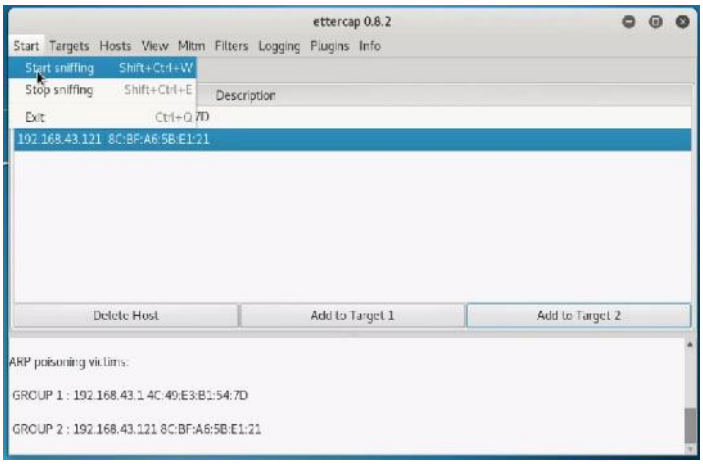
Gambar 3.8. Menambahkan IP Korban sebagai Target 2

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



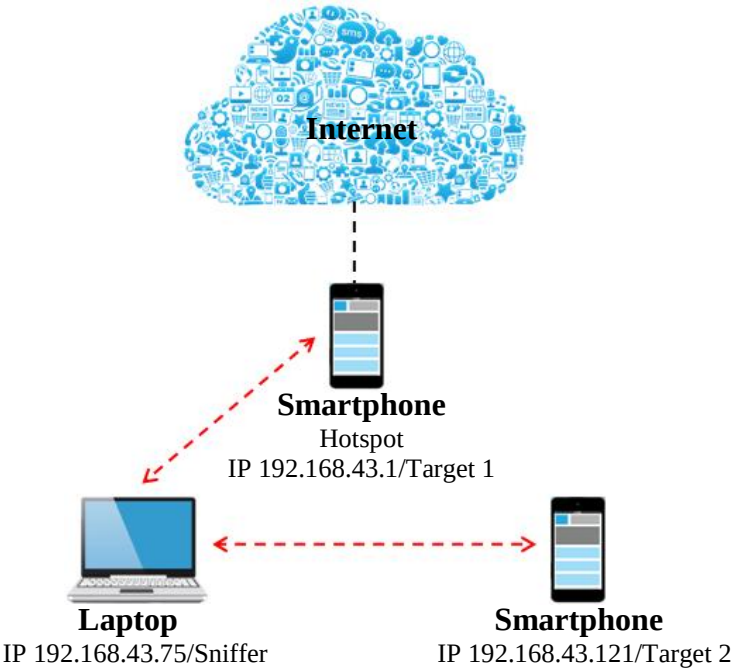
Gambar 3.9. MITM *Attack*: ARP *Poisoning*

9. Mengklik “Ok”, Kemudian menjalankan *sniffing* dengan cara mengklik menu “*Start*” kemudian pilih “*Start sniffing*”.



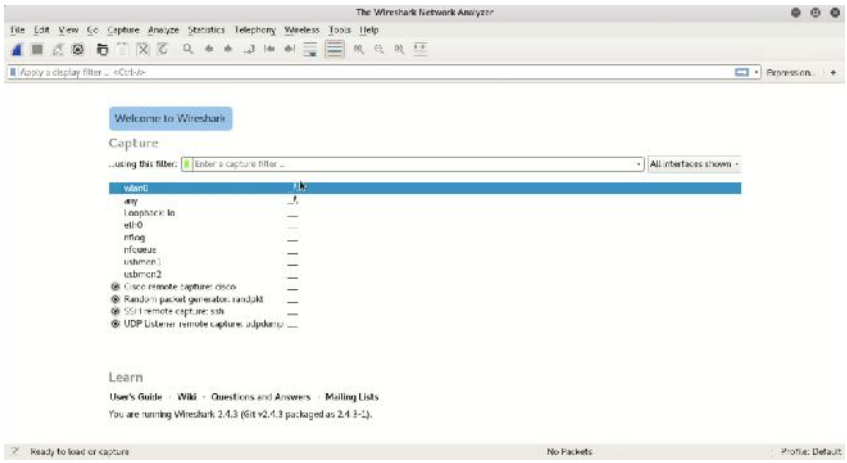
Gambar 3.10. Memulai Proses *Sniffing*

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

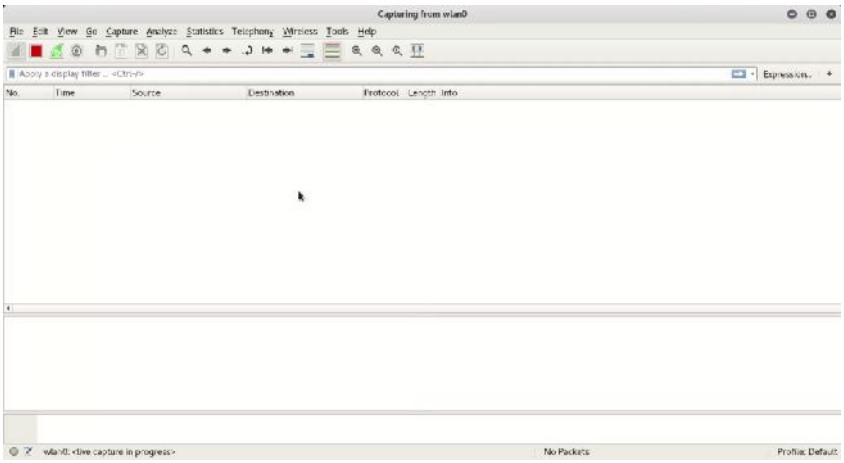
10. Membuka Wireshark, pada Kali Linux pilih "*Aplications*" kemudian "*Sniffing & spoofing*" lalu pilih "Wireshark", maka akan muncul tampilan awal aplikasi Wireshark seperti gambar berikut.



Gambar 3.12. Tampilan Awal Aplikasi Wireshark

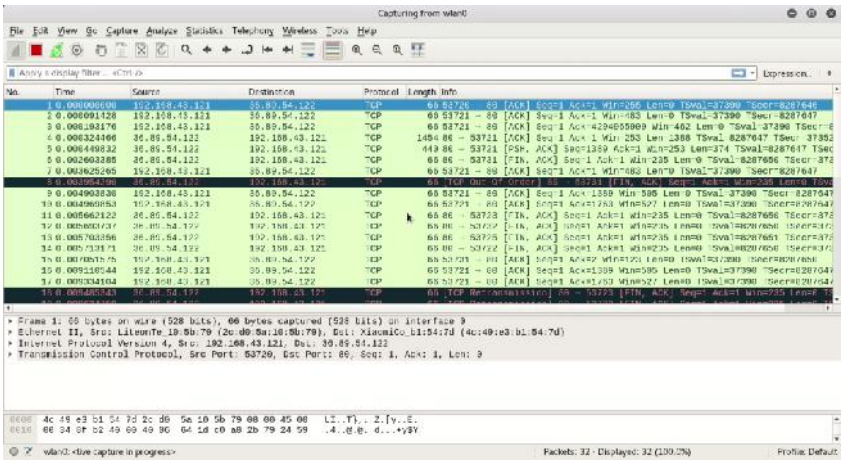
11. Kemudian masuk ke dalam *interface* yang memiliki paket data pada jaringan yang ditandai dengan adanya diagram gelombang. Pada kausus ini penulis

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



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.



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.

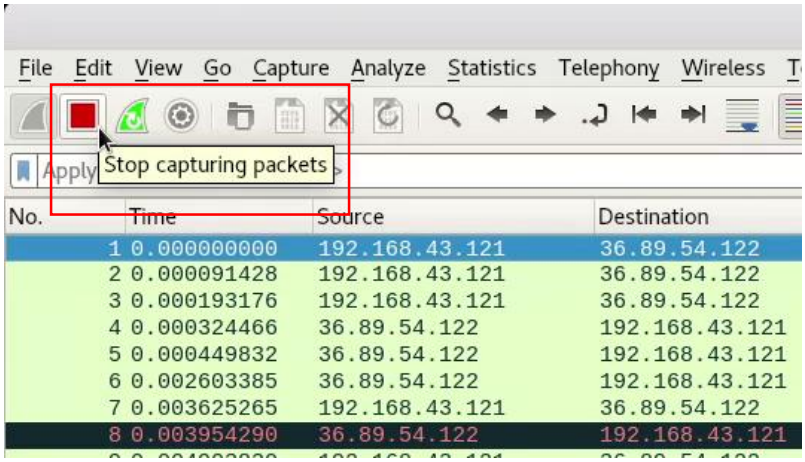
Gambar 3.16. Google Chrome Menolak Koneksi

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.



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 :

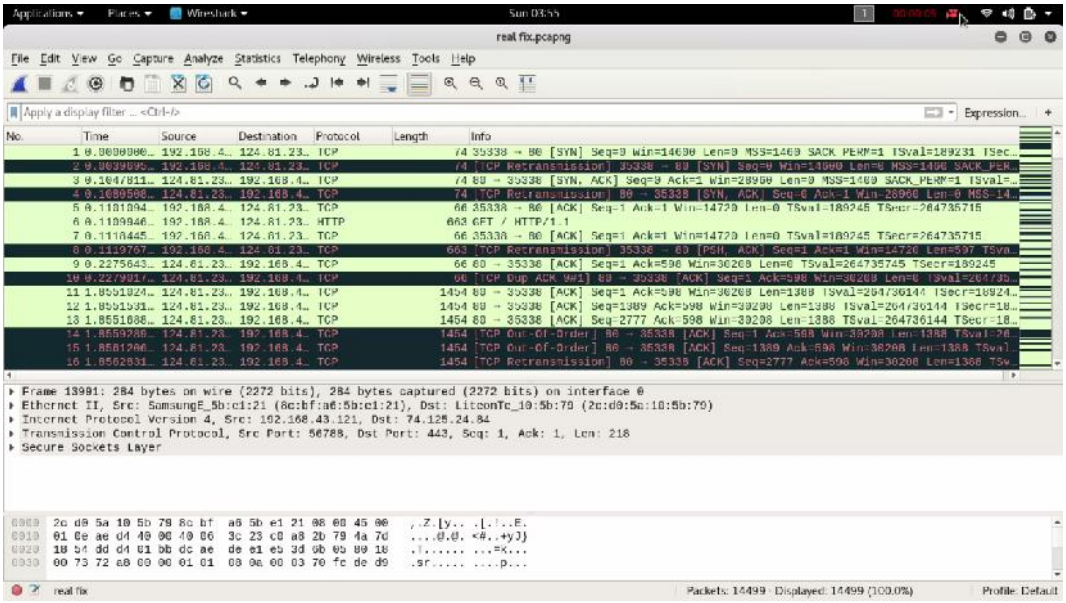
1. Skenario Pertama pada *Website* Simak Unismuh

- 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.

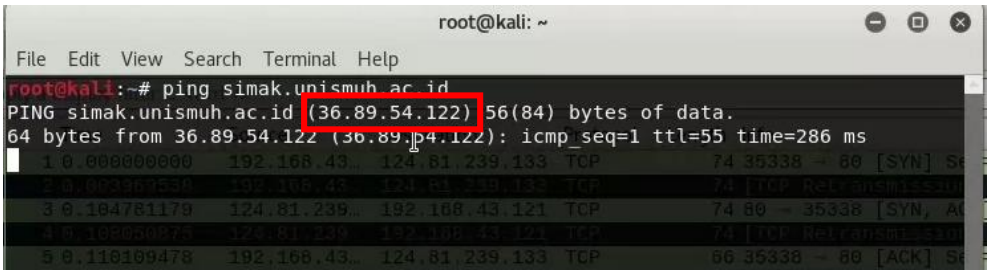


Gambar 4.1 Hasil Rekaman Paket Data

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

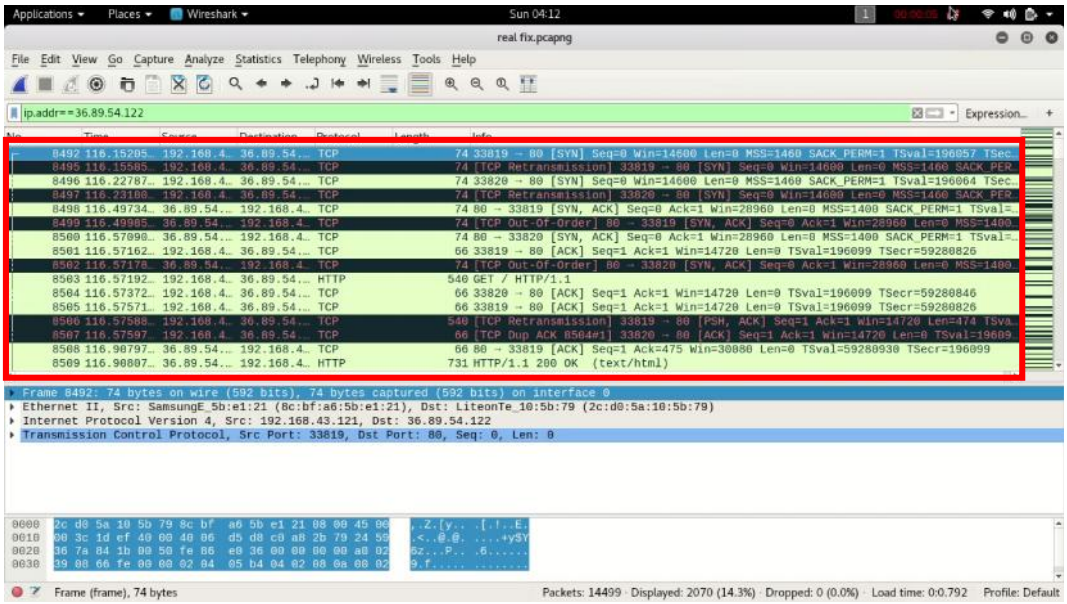
Untuk melihat paket yang berasal dari *website* Simak Unismuh, maka diharuskan melakukan penyaringan dahulu dari paket yang telah direkam. Sebelum melakukan penyaringan terlebih dahulu, penulis harus mengetahui IP *address* dari *website* Simak Unismuh yang memiliki DNS "simak.unismuh.ac.id" dengan cara 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.



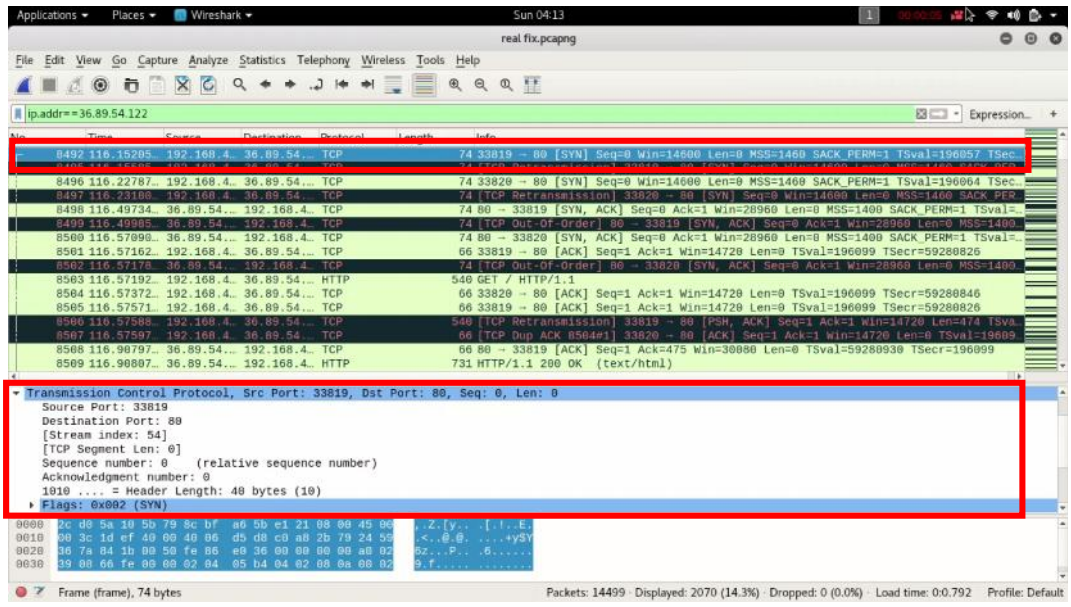
Gambar 4.3. Hasil Penyaringan Paket Data simak.unismuh.ac.id

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.



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

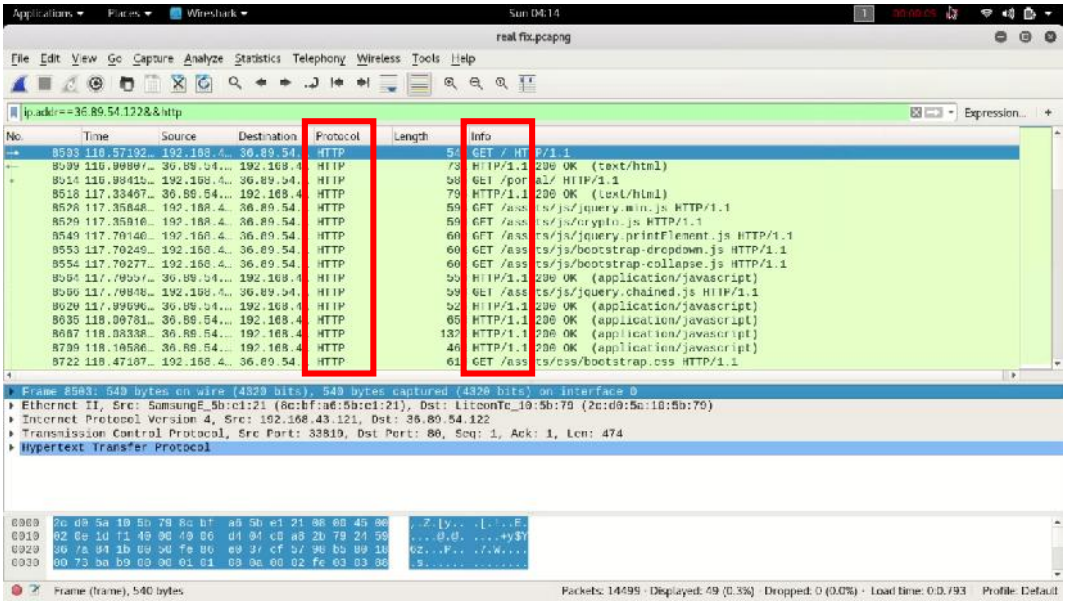
- *Destination Port* : http (80)

  Menunjukkan *port* yang digunakan server adalah 80 yaitu http.

- *Flags*: 0x002 (SYN)

  Menunjukkan *client* ingin meminta data dari server.

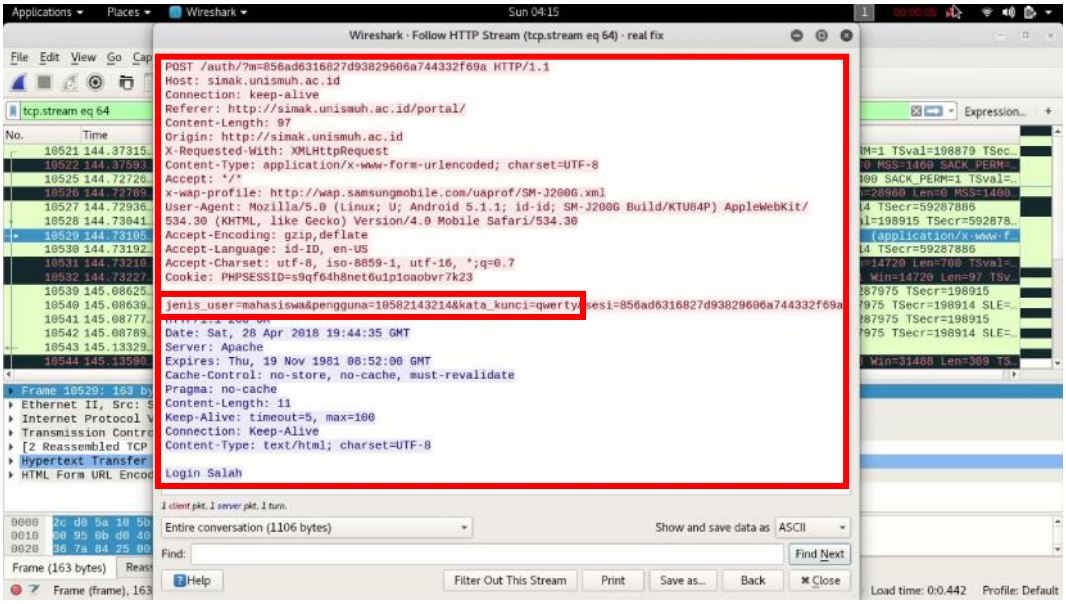
Karena dalam penelitian ini hanya menganalisis keamanan *website*, maka penulis melakukan penyaringan lagi dengan mengetik perintah “ip.addr==36.89.54.122&&http" maka akan tampil paket-paket yang memiliki protokol HTTP seperti pada gambar berikut.



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.

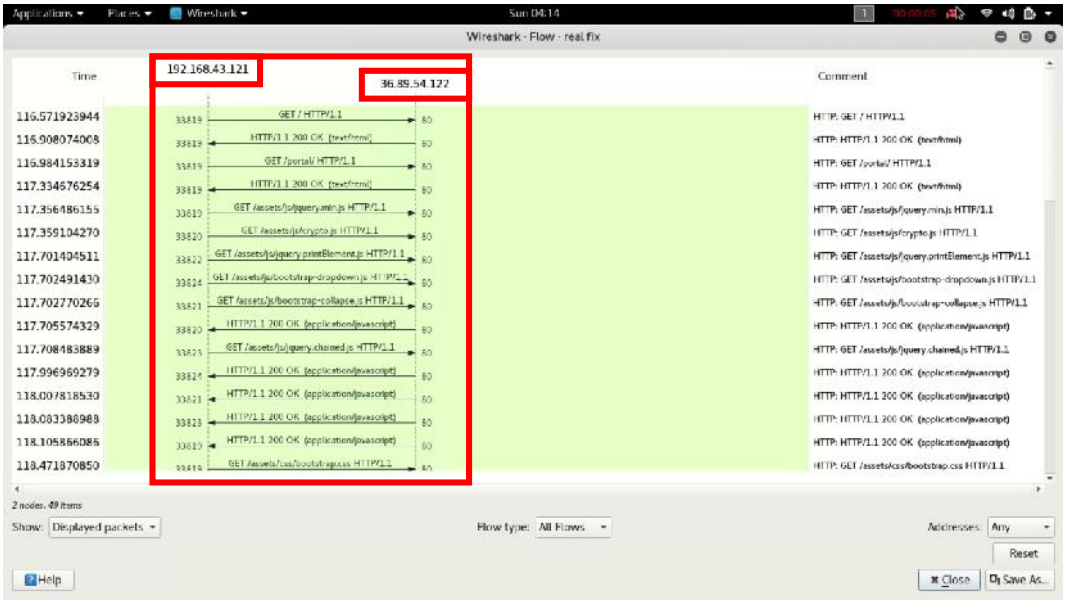
- Date: Sat, 28 Apr 2018 19:44:35 GMT.

  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.



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:

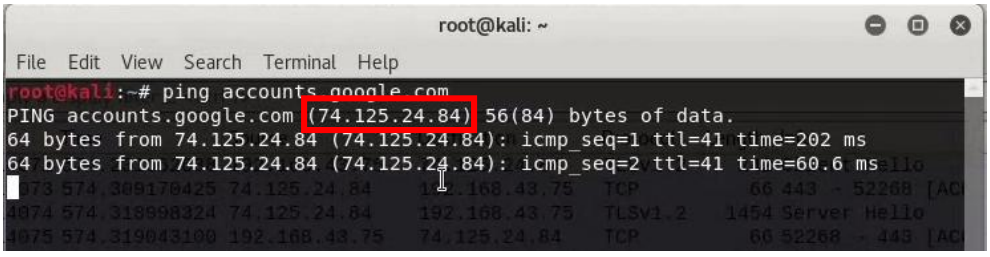
~ *Username* : hasbullah.jj@gmail.com.

~ *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.

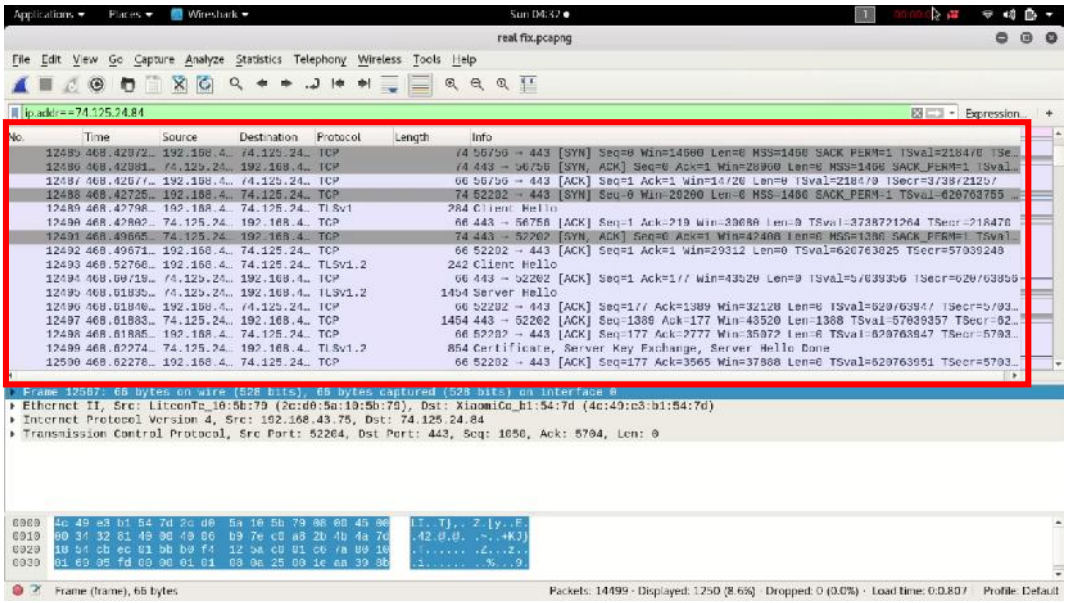
Untuk melihat paket yang berasal dari *website* Google Accounts, maka harus melakukan penyaringan dahulu dari paket yang telah direkam. Sebelum melakukan penyaringan terlebih dahulu, penulis harus mengetahui IP *address* dari *website* Google Accounts yang memiliki DNS "accounts.google.com" dengan cara 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.



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.



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

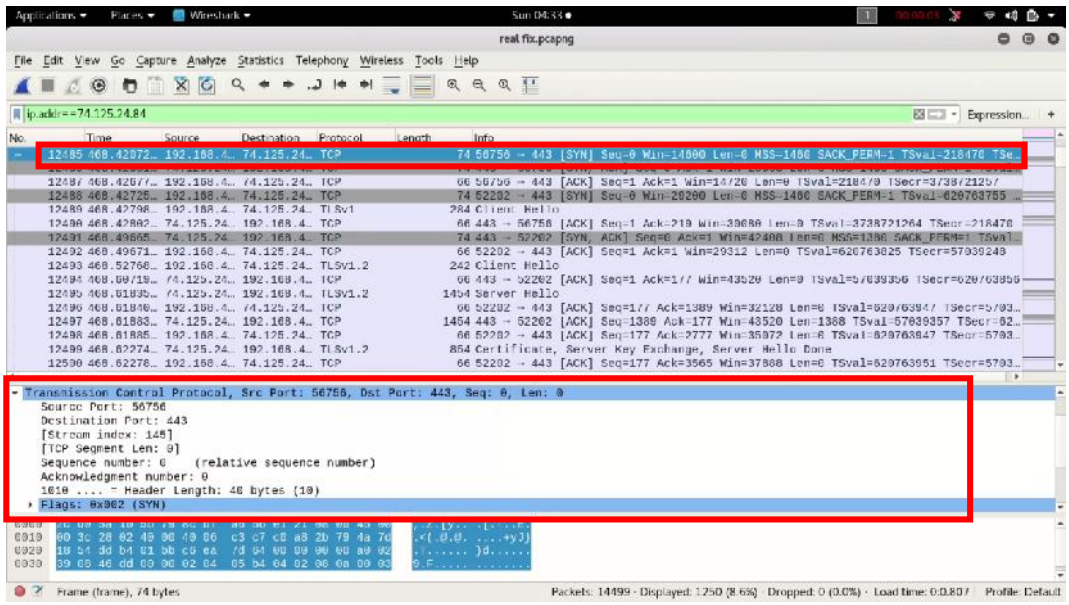
Pada Gambar 4.9 merupakan seluruh paket data yang memiliki IP *Address* 74.125.24.84 yang terdapat pada *Source* ataupun pada *Destination*.

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.



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

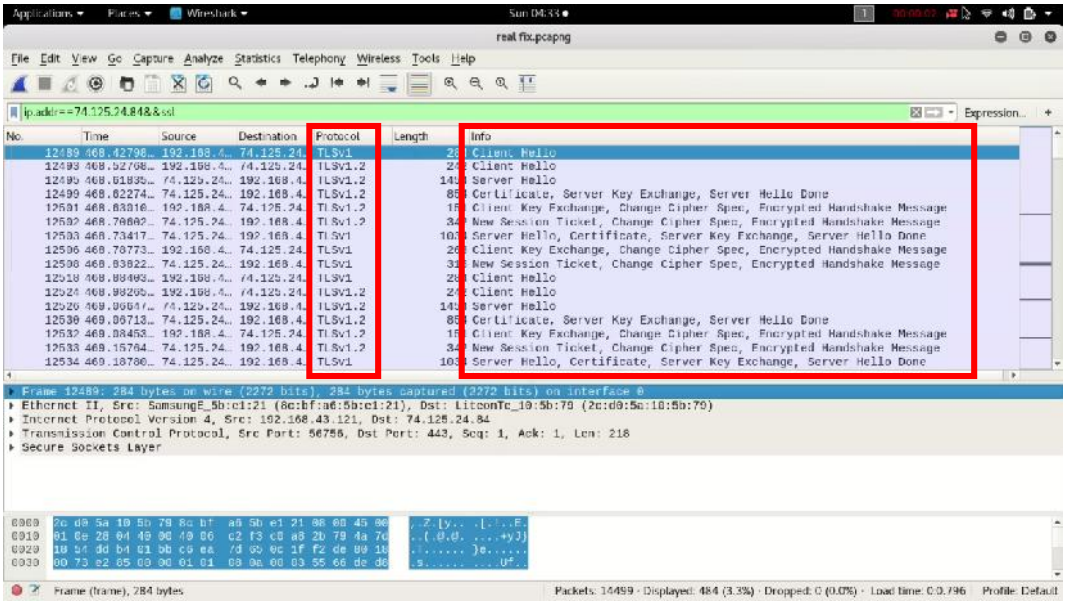
- *Destination Port* : 443

  Menunjukkan *port* yang digunakan server adalah 443 yaitu https.

- *Flags*: 0x002 (SYN)

Menunjukkan *client* ingin meminta data dari server.

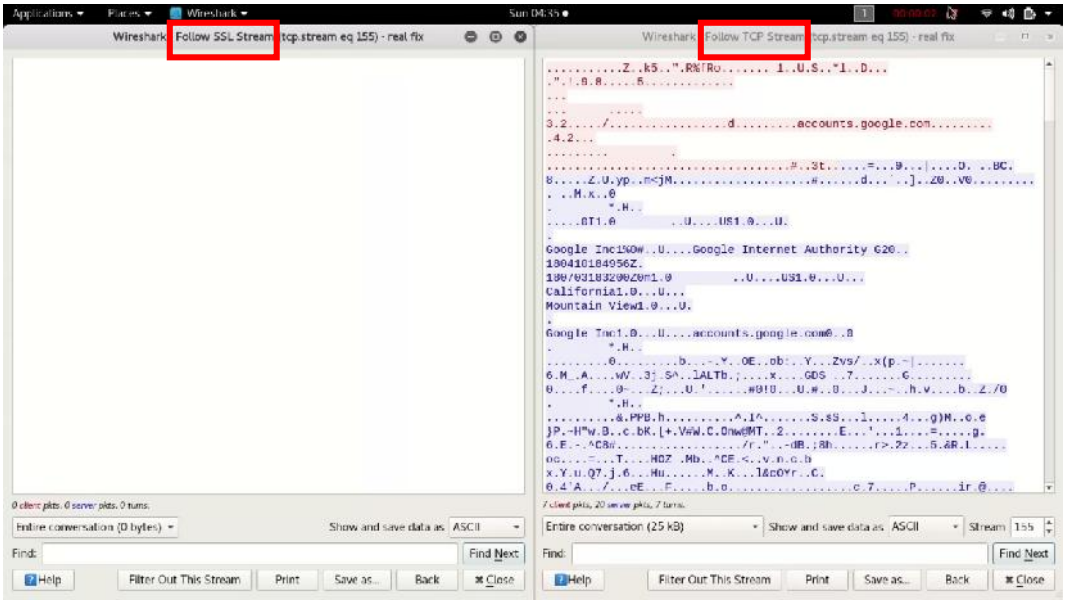
Karena dalam penelitian ini hanya menganalisis keamanan *website*, maka penulis melakukan penyaringan lagi dengan mengetik perintah “ip.addr==74.125.24.84&&ssl" maka akan tampil paket-paket seperti pada gambar berikut.



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*.

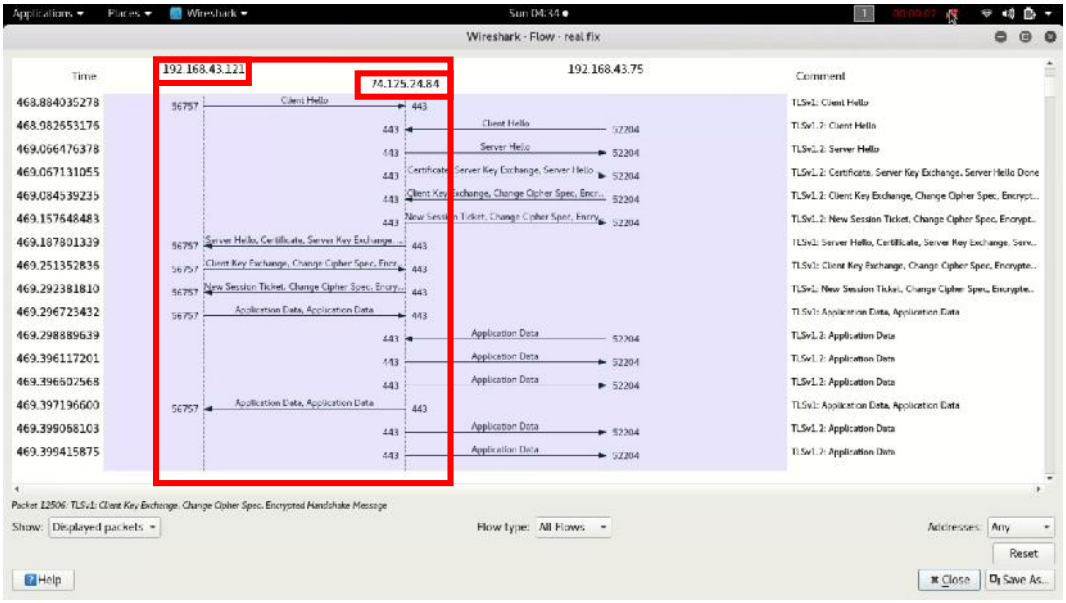
Untuk menganalisisnya dapat dilakukan dengan cara mengklik kanan pada paket data yang ingin dianalisis kemudian pilih *Follow* SSL *Stream*. Berikut adalah salah satu tampilan *detail packet* data protokol TLS yang memiliki info *Application Data*.



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.

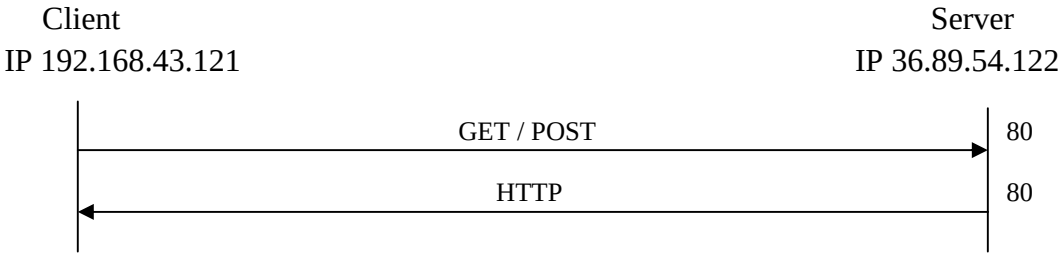
B. Pembahasan

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.



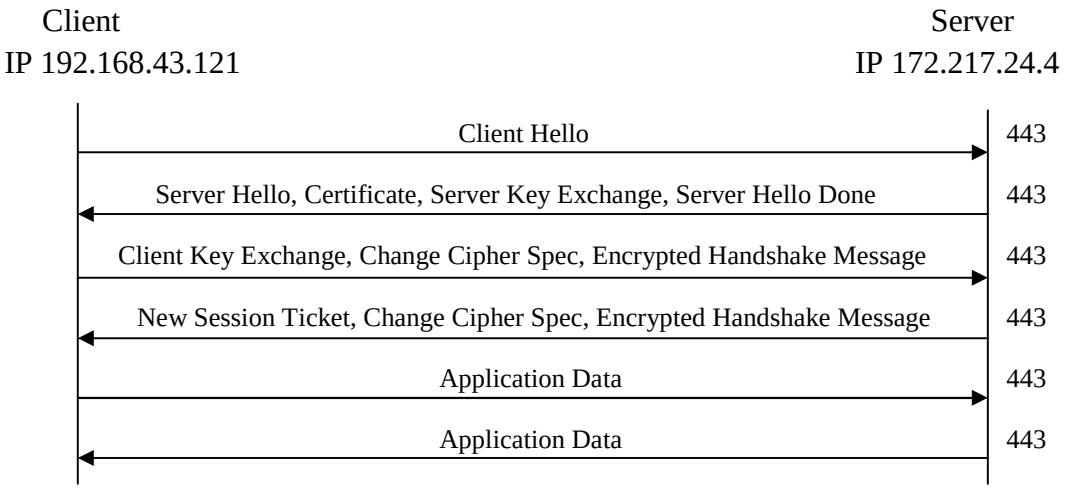
Gambar 4.14. Proses Komunikasi Data *Website* Simak Unismuh

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 *plain-text*.

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.



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 *client* untuk menunjukkan bahwa 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 dapat mengirim data aplikasi melalui saluran aman yang telah *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:

1. 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 http://www.trijurnal.lemlit.trisakti.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 https://ejournal.fikom-unasman.ac.id/index.php/jikom/article/view/34.

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 http://repo.polinpdg.ac.id/273/.

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 https://jurnalinforman.wordpress.com/2013/03/30/analisis-keamanan-sistem-login/.

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 http://ejournal.uin-suska.ac.id/index.php/SNTIKI/article/view/3368.

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 http://eprints.binadarma.ac.id/2404/.

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 http://pulungan.staff.ugm.ac.id/pubs/RP-KNSI-11.pdf.

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 http://www.unisbank.ac.id/ojs/index.php/fti1/article/view/33.

Wikipedia. (2018, Januari 5). Ensiklopedia Bebas. *Transport Layer Security* ,Diakses pada 11:50, Januari 5, 2018, dari https://id.wikipedia.org/w/index.php?title=Transport_Layer_Security&oldid=13502518

Wikipedia. (2018, Februari 15). Ensiklopedia Bebas. *Situs Web*, Diakses pada 15:38, Februari 15, 2018, dari https://id.wikipedia.org/w/index.php?title=Situs_web&oldid=13705588.

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.

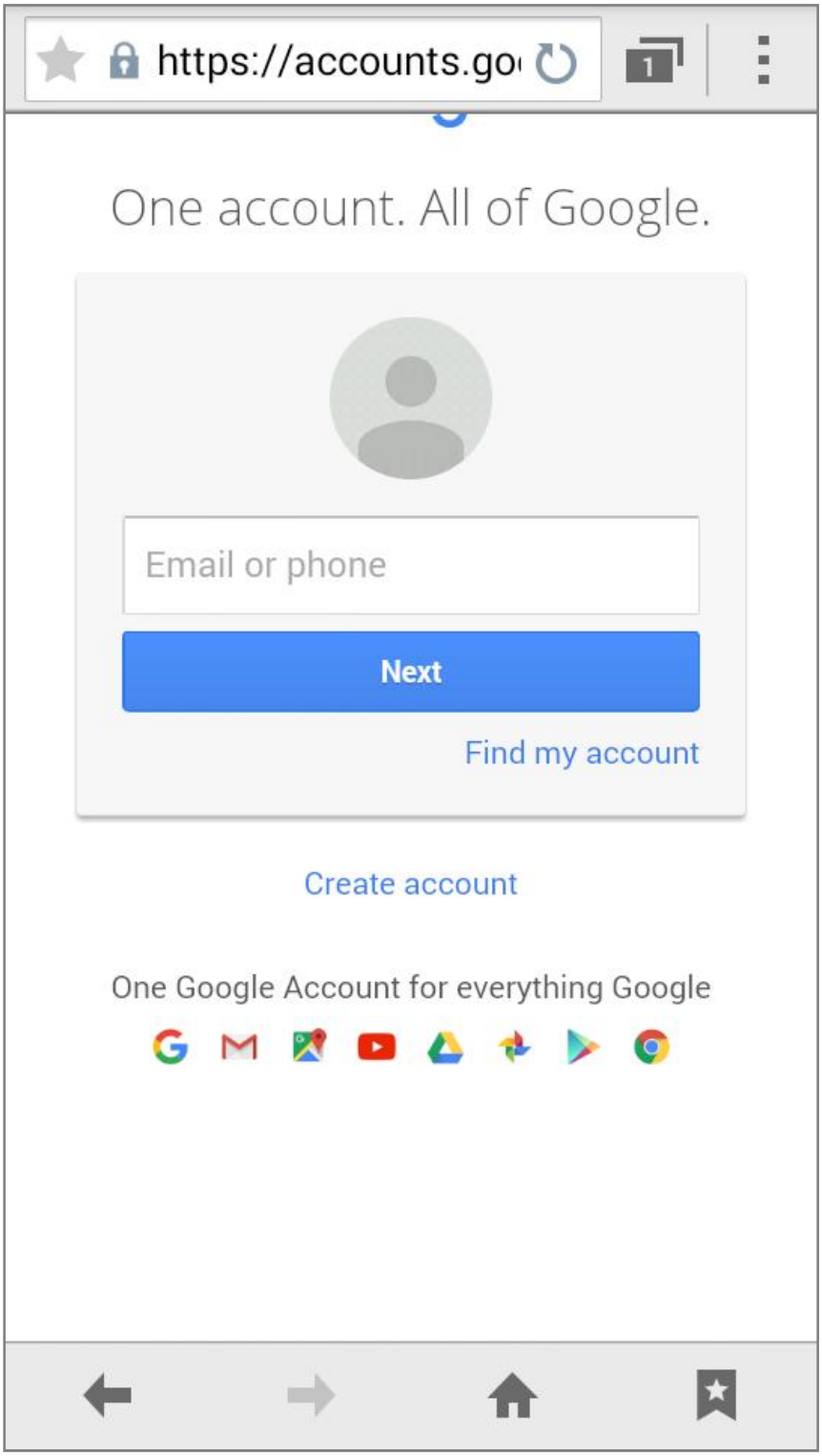
Zam, E. (2016). *Buku Sakti Wireless Hacking*, PT Elex Media Komputindo, Jakarta.

LAMPIRAN

LAMPIRAN 1

Tampilan Halaman *Website*

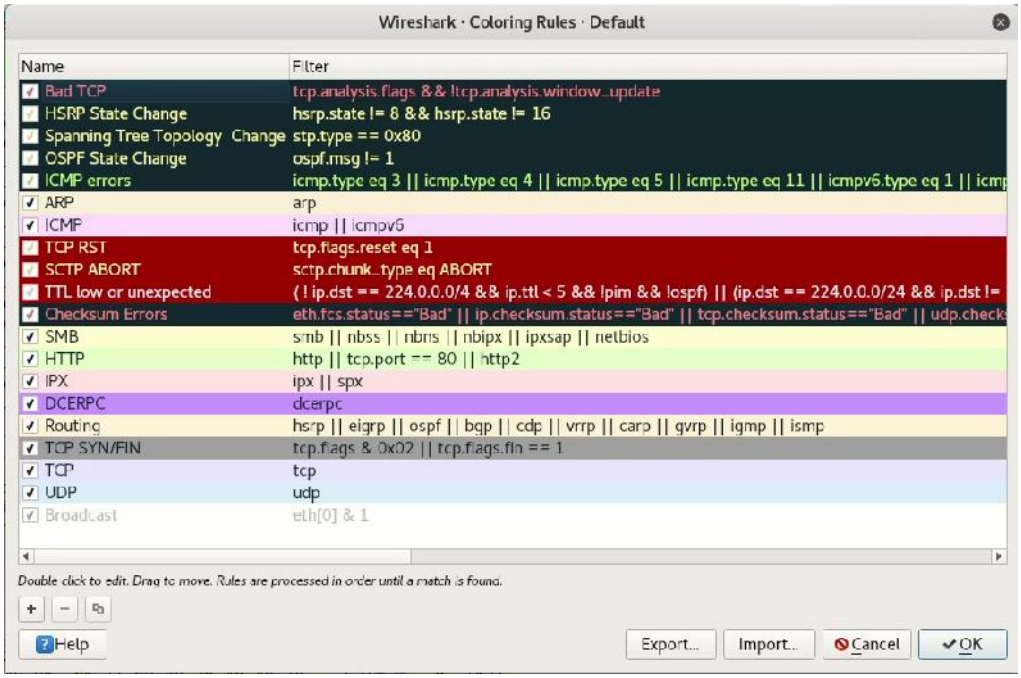
Gambar L1-1. Halaman *Website* Simak Unismuh



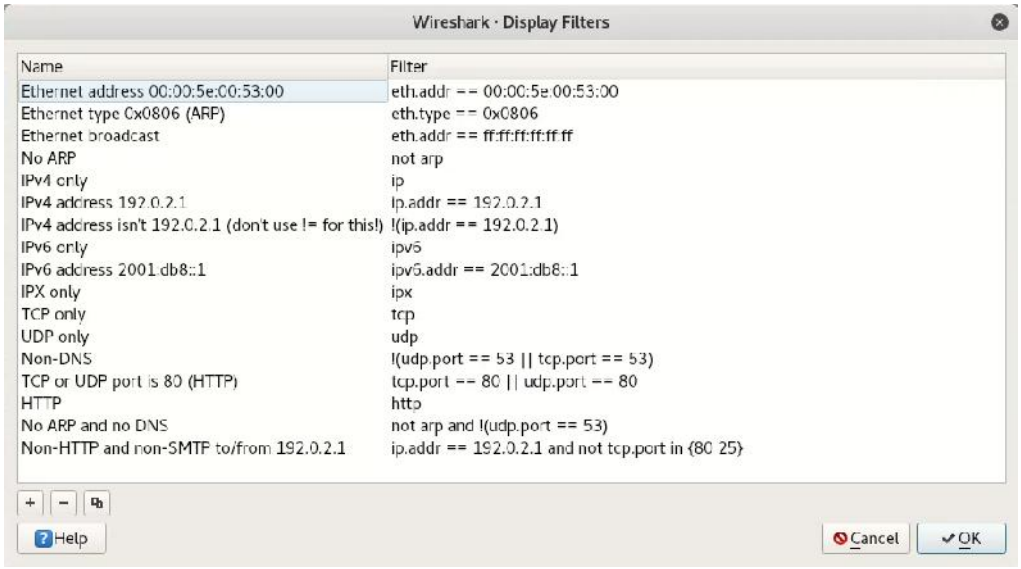
Gambar L1-2. Halaman *Website* Google Accounts

LAMPIRAN 2

Dialog Box sebagai Data Tambahan untuk Menganalisis Paket Data pada Aplikasi Wireshark



Gambar L2-1. *Coloring Rules* Wireshark



Gambar L2-2. *Display Filter* Wireshark

LAMPIRAN 3

Surat Penelitian

UNIVERSITAS MUHAMMADIYAH MAKASSAR
FAKULTAS TEKNIK
GEDUNG MENARA IQRA LT. 3
Jl. Sultan Alauddin No. 259 Telp. (0411) 866 972 Fax (0411) 865 588 Makassar 90221
Website: www.unismuh.ac.id, e_mail: unismuh@gmail.com
Website: http://teknik.unismuh.makassar.ac.id

بسم الله الرحمن الرحيم

Nomor : 216/05/C.4-VI/IV/39/2018 Makassar, 10 Sya'ban 1439 H
Lamp. : - 26 April 2018 M
Hal : **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 :

Nama	: **Hasbullah Jamaluddin (105 82 1404 141432 14)**
	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.

Jazakumullah Khaeran Katsiran
Wassalamu 'Alaikum warahmatullah Wabarakatuh

Dekan,

Ir. Hamzah Al Imran, S.T., M.T.
NBM. 855 500

Tembusan: 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