ISBN : 978-623-7297-39-0

# IMPLEMENTASI APLIKASI *CAIN AND ABEL* DALAM PENYADAPAN PAKET DATA PADA JARINGAN *WIFI*

**Muhammmad Huzaifah Nasution, Khairuddin Nasution, Oris Krianto Sulaiman**
Program Studi Teknik Informatika, Fakultas Teknik Universitas Islam Sumatera Utara
*mhdhuzaifahnst@gmail.com; khairudin33@gmail.com; oris.ks@ft.uisu.ac.id*

**Abstrak**

*Penggunaan Fasilitas wifi telah menjadi kebutuhan bagi setiap orang, dengan wifi kita bisa langsung menghubungakan koneksi ke internet untuk kebutuhan transfer data, browsing, atau yang lainnya. Oleh karena itu, pengetahuan ketidakamanan jaringan wifi juga sangat dibutuhkan untuk lebih berhati – hati dalam menjaga data agar terhindar dari serangan pencurian data privasi yang sangat sering terjadi. Oleh karena itu dilakukan pecobaan penyadapan menggunakan aplikasi cain and abel di fasilitas wifi Fakultas Teknik UISU, untuk membuktikan ketidakamanan data ketika terhubung di jaringan wifi dan memberitahukan kenggunaan dasar aplikasi cain and abel. Hasil yang didapat dari penelitian ini adalah, aplikasi cain and abel dapat menyadap paket data pada protokol http dan tidak dapat menyadap paket data pada protokol https.*

**Kata-Kata Kunci :** *Keamanan Data, Wifi, Penyadapan, Cain and Abel*

## I. PENDAHULUAN

Saat ini kemajuan teknologi sangat berkembang pesat. Keamanan jaringan menjadi sangat penting dan harus diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat dicuri datanya oleh para *cracker*, baik jaringan LAN maupun *Wireless*. Pada saat data dikirim melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan kepada user lain yang tidak bertanggung jawab untuk menyadap atau mengubah data, bahkan sampai mencuri data tersebut. Dalam pembangunan perancangannya, sistem keamanan jaringan yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh para *hacker* maupun *cracker*. Beberapa aksi *sniffing* lebih menakutkan lagi, biasanya *cracker* melakukan *sniffing* ditempat rawan, misalnya seorang user melakukan sniffing di universitas tempat belajar, atau seorang *cracker* melakukan *sniffing* untuk mencuri password email, bahkan mencuri data transaksi melalui kartu kredit maupun hal lainnya. Pada kenyataanya, masih sedikit solusi yang tepat untuk mendeteksi maupun untuk mencegah aktivitas *sniffing* ini. Sistem deteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai serangan tetapi tidak mengambil tindakan lebih lanjut.

Internet adalah tempat yang terbuka untuk tersampainya bermacam informasi. Tapi dibalik keterbukaan informasi yang memudahkan itu juga terdapat resiko dan bahaya dan risiko yang mengancam, antara lain terganggunya privasi dan kerahasiaan pribadi penggunanya, yang mungkin tidak seharusnya diketahui oleh orang lain. Mengingat banyaknya upaya, *malware*, virus, *hacker* atau sekedar orang iseng, kita dituntut untuk mewaspadai keamanan informasi pribadi kita di dunia maya.

Permasalahan yang terjadi saat ini pada penulis dan sebagian besar pengguna internet hanya sekedar menggunakannya saja, tanpa memperhatikan keamanan data privasi ketika menggunakan internet, sehingga data privasi pengguna tersebut mudah diketahui oleh orang yang tidak beretika dalam bidang IT.

## II. TINJAUAN PUSTAKA

### 2.1 Paket *Sniffer*

Menurut Lutfi Nur Niswati. (2013). *Paket Sniffer* (arti tekstual: pengendus paket dapat pula diartikan ‘penyadap paket’) yang juga dikenal sebagai Network *Analyzers* atau *Ethernet Sniffer* ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak-balik pada jaringan, aplikasi ini menangkap tiap-tiap paket dan kadang-kadang menguraikan isi dari RFC (*Request for Comments*) atau spesifikasi yang lain. Berdasarkan pada struktur jaringan (seperti hub atau switch), salah satu pihak dapat menyadap keseluruhan atau salah satu dari pembagian lalu lintas dari salah satu mesin di jaringan.

Perangkat pengendali jaringan dapat pula diatur oleh aplikasi penyadap untuk bekerja dalam mode campur-aduk *(promiscuous mode)* untuk “mendengarkan” semuanya (umumnya pada jaringan kabel).

*Packet sniffer* adalah sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun *nirkabel*. Setelah paket - paket yang lewat itu didapatkan, paket - paket tersebut kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang. Hal ini dapat dilakukan karena pada dasarnya semua koneksi *ethernet* adalah koneksi yang bersifat broadcast, di mana semua host dalam sebuah kelompok jaringan akan menerima paket yang dikirimkan oleh sebuah host. Cukup sulit untuk melindungi diri dari gangguan ini karena sifat dari packet *sniffing* yang merupakan metode pasif (pihak

penyerang tidak perlu melakukan apapun, hanya perlu mendengar saja).

### 2.2 Aplikasi *Cain and Abel*

Menurut ilmukomputer.com, program bantu *cain & abel* merupakan program hasil buah karya Massimiliano Montoro. Program ini dikhususkan dalam penanganan *recovery password* pada *system operasi Microsoft Windows* yang cenderung menangani masalah jaringan (baik aplikasi *networking* sampai dengan aplikasi yang menggunakan fitur *database server*), dan aplikasi ini dapat membantu dalam pegujian keamanan jaringan pada sebuah *website*.

### 2.3 Pengertian Wifi

Menurut www.yuksinau.id (2021), Secara umum, pengertian *Wifi* adalah teknologi untuk saling bertukar data menggunakan gelombang radio (secara nirkabel) dengan memanfaatkan berbagai peralatan elektronik. Diperlukan peralatan elektronik seperti misalnya komputer, *smartphone*, tablet, atau bahkan video game console untuk terhubung dalam jaringan komputer, termasuk internet, melalui *Wifi*. titik akses memiliki jangkauan hingga 20 meter di dalam ruangan, dan ada pula yang lebih jauh jangkauannya untuk *Wifi* di luar ruangan.

### 2.4 *Hypertext Transfer Protokol* (HTTP)

Menurut beon.co.id, *Hypertext Transfer Protokol* adalah adalah sebuah protokol jaringan lapisan aplikasi yang digunakan untuk sistem informasi terdistribusi, kolaboratif, dan menggunakan *hipermedia* penggunaannya banyak pada pengambilan sumber daya yang saling terhubung dengan tautan yang disebut dengan dokumen *hiperteks* yang kemudian membentuk *World Wide Web* pada tahun 1990 oleh fisikawan inggris yang bernama Tim Berners Lee. Http merupakan protokol yang menyediakan perintah dalam komunikasi antar jaringan, yaitu komunikasi antara jaringan komputer *client* dengan web server. Dalam komunikasi ini, komputer *client* melakukan permintaan dengan mengetikkan alamat atau *website* yang ingin di akses. Sedangkan server mengolah permintaan tersebut berdasarkan kode protokol yang di inputkan.

### 2.5 *Hypertext Transfer Protokol Secure* (HTTPS)

Menurut beon.co.id, *Hypertext Transfer Protocol Secure* memiliki pengertian yang sama dengan http hanya saja https memiliki kelebihan fungsi di bidang keamanan (*secure*). Dengan menggunakan *Secure Socket Layer* (SSL) atau *Transport Layer Security* (TLS) sebagai sublayer di bawah http aplikasi layer yang biasa. Teknologi https protokol mencegah kemungkinan "dicurinya" informasi penting yang dikirimkan selama proses komunikasi berlangsung antara user dengan web server atau sebaliknya. Secara teknis, website yang menggunakan https akan melakukan enkripsi terhadap informasi (data) menggunakan teknik enkripsi SSL. Dengan cara ini meskipun seseorang berhasil "mencuri" data tersebut selama dalam perjalanan user web server, orang tersebut tidak akan bisa membacanya karena sudah diubah oleh teknik enkripsi SSL. Umumnya website yang menggunakan https ini adalah website yang memiliki tingkat kerawanan tinggi yang berhubungan dengan masalah keuangan dan privasi dari pelanggannya seperti website perbankan dan investasi. HTTPS dienkripsi dan deskripsi dari halaman yang di minta oleh pengguna dan halaman yang di kembalikan oleh web server. Kedua protokol tersebut memberikan perlindungan yang memadai dari serangan *eavesdroppers*, dan *man in the middle attacks*. Pada umumnya port yang digunakan HTTPS adalah port 443.

### 2.6 Pengetian Website

Menurut Dina Fitria Murad dkk website adalah sebuah sistem dengan informasi yang disajikan dalam bentuk teks, gambar, suara, dan lainnya yang tersimpan dalam sebuah server web internet yang disajikan dalam bentuk *hyper teks* (Murad, Kusniawati, Asyanto, 2013).

## III. METODE PENELITIAN

Metode penelitian ini merupakan suatu cara yang dilakukan dalam penelitian sehingga pelaksanaan dan hasil penelitian dapat di tanggung jawabkan secara ilmiah.

Dalam penelitian ini terdiri dari beberapa tahapan yaitu :

**A. Studi pustaka**

Dalam melakukan pengumpulan data, penulis menggunakan teknik studi pustaka. Pada tahapan pengumpulan data dengan cara studi pustaka, penulis mencari referensi-referensi yang relevan dengan objek yang akan diteliti. Pencarian referensi dilakukan di perpustakaan, maupun secara *online* melalui internet. Setelah mendapatkan referensi-referensi yang relevan tersebut, penulis lalu mencari informasi- informasi yang dibutuhkan dalam penelitian ini dari referensi-referensi tersebut. Informasi yang didapatkan digunakan dalam penyusunan landasan teori, metodologi penelitian serta pengembangan aplikasinya secara langsung. Pustaka-pustaka yang dijadikan acuan dapat dilihat di Daftar Pustaka.

**B. Pengumpulan *hardware* dan *software***

Menyiapkan hardware dan software yang dibutuhkkan untuk menunjang pelaksanaan penelitian seperti :

- Dua buah laptop core i3
- Satu buah wifi
- OS windows 7
- *Google chrome*
- Aplikasi *cain and abel*
-

**C. konfigurasi *hardware* dan *software***

Melakukan konfigurasi *hardware* dan *software* seperti :

- Menghidupkan laptop dan menghubungkannya pada sebuah wifi di Fakultas Teknik UISU.
- Mengidentifikasi *wifi*.
- Menjalankan aplikasi *cain and abel*.
- membuka *google chrome* pada laptop client dan mencoba login pada *website* http.
- membuka *google chrome* pada laptop client dan mencoba login pada website https.

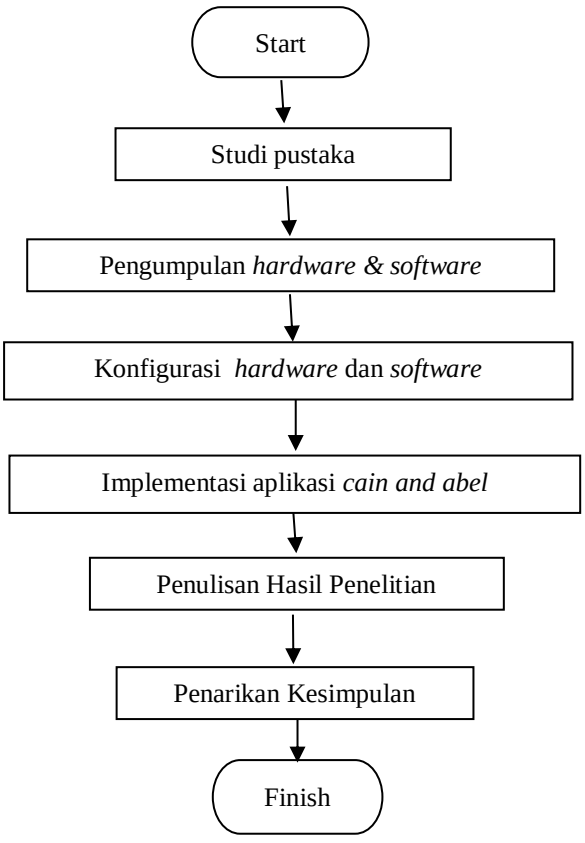
**D. Implementasi aplikasi *cain and abel***

Melakukan percobaan penyadapan paket data sebagai berikut :

- Configurasi aplikasi *cain and abel* pada mode *sniffing*.
- Melihat hasil yang di peroleh dari percobaan penyadapan paket data pada *website* http di aplikasi *cain and abel*.
- Melihat hasil yang di peroleh dari percobaan penyadapan paket data pada *website* https di aplikasi *cain and abel*.

**E. Penulisan hasil penelitian.**

Menuliskan hasil pengujian aplikasi *cain and abel* pada jaringan *wifi* Fakultas Teknik UISU.




**Gambar 1. *Flowchart* Tahapan Penelitian**

## IV. HASIL DAN PEMBAHASAN

### 4.1 Mengidentifikasi *Wifi*

Percobaan ini dilakukan untuk mengidentifikasi *wifi* dalam bentuk informasi lengkap dengan nama SSID, *gateway*, dan *security* atau keamanan yang digunakan.

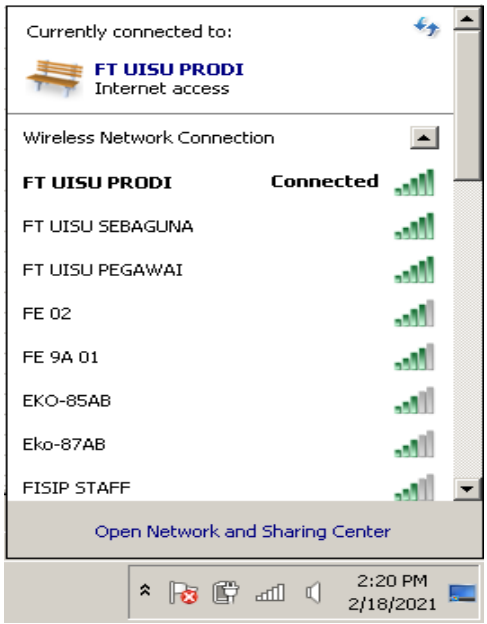
Adapun hasil yang di dapat dari identifikasi tersebut adalah :

**Tabel 1. Hasil Identifikasi *Wifi***

| Nama *Wifi* (SSID) | *Gateway* | Jenis Keamanan |
|---|---|---|
| **FT UISU PRODI** | 192.168.90.254 | WPA2 – PSK |

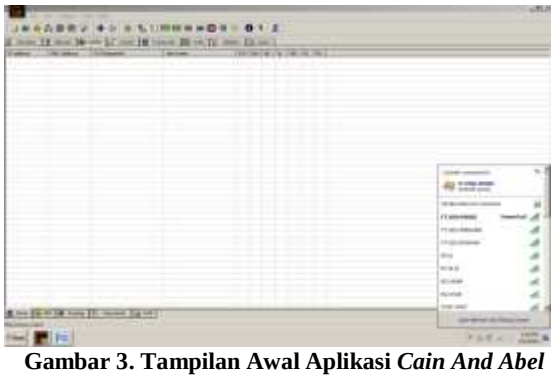
### 4.2 Percobaan penyadapan paket data pada SSID FT UISU PRODI

1. Menghubungkan laptop pada *wifi* FT UISU PRODI.



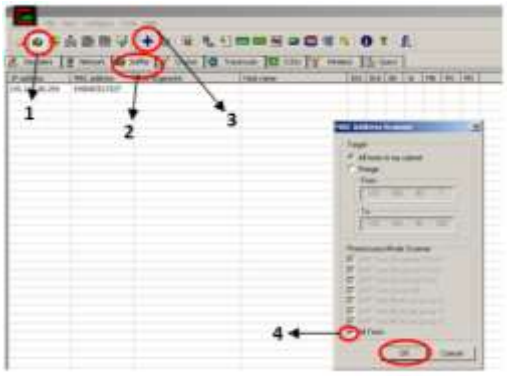

**Gambar 2. Laptop Terhubung Pada *Wifi* FT UISU PRODI.**

2. Buka Aplikasi *Cain And Abel*.



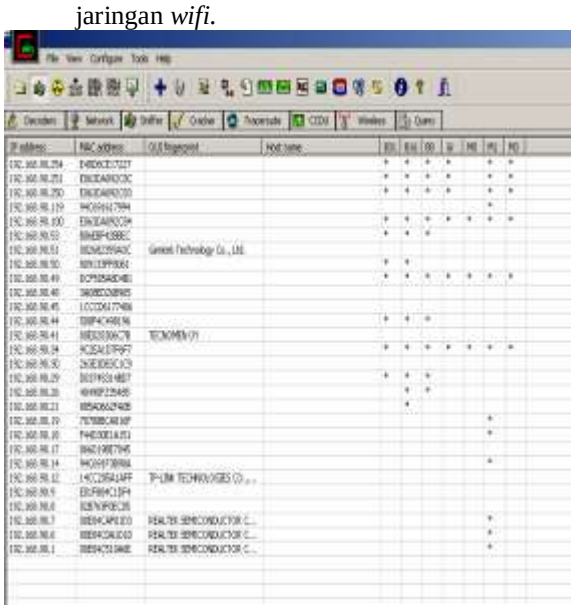
**Gambar 3. Tampilan Awal Aplikasi *Cain And Abel***

3. - Pertama, klik start/stop *sniffer*.
   - Kedua, klik *sniffer*.
   - Ketiga, klik *add to list.*
   - Kempat, klik *all tests*, kemudian klik ok.



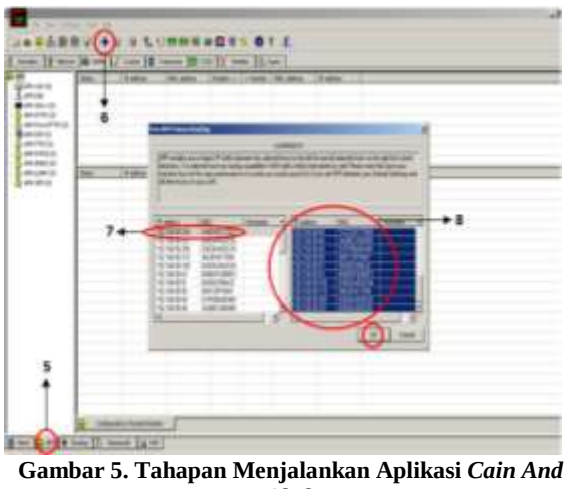

**Gambar 3. Tahapan Menjalankan Aplikasi *Cain And Abel***

4. Akan tampil seluruh ip yang tehubung pada jaringan *wifi.*



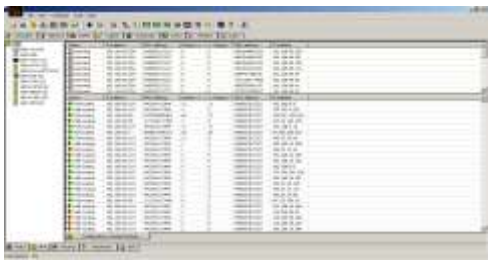
**Gambar 4. Tampilan seluruh ip yang tehubung pada jaringan *wifi.***

5. - Kelima, klik APR.
   - Keenam, klik *add to list.*
   - Ketujuh, klik ip *gateway* 192.168.90.254
   - Kedelapan, *shift* seluruh ip target, kemudian klik ok.




**Gambar 5. Tahapan Menjalankan Aplikasi *Cain And Abel.***

6. Kemudian klik *start/stop* APR, lalu akan muncul tampilan seperti gambar 4.5, (proses penyadapan paket data sedang berlangsung).



**Gambar 6. Tampilan proses penyadapan paket data sedang berjalan**

7. Kemudian *login* pada sebuah *website* dengan protokol http, (http://repository.usu.ac.id/password-login).


**Gambar 7. *login* pada *website* dengan protokol http**

8. Klik tombol *password*, kemudian akan tampil informasi *login* pengguna *wifi.*

**Gambar 8. Hasil percobaan penyadapan paket data pada protokol http.**

9. Kemudian *login* pada sebuah *website* dengan protokol https, (https://dashboard.prakerja.go.id/masuk).


**Gambar 9. *login* pada *website* dengan protocol https**

ISBN : 978-623-7297-39-0

10. Aplikasi *cain and abel* tidak dapat menangkap paket data pada protokol https.

**Gambar 10. Hasil percobaan penyadapan paket data pada protokol https.**

### 4.3 Pembahasan

Dari percobaan di atas didapatkan hasil sebagai berikut :

Aplikasi *cain and abel* dapat menyadap paket data berupa *username* dan *password* pada *website* dengan protkol http saja, sementara dapat dilihat dari hasil percobaan di atas aplikasi *cain and abel* tidak mampu menangkap paket data pada *website* dengan protokol https, dianjurkan kepada pengelola *website* dengan protokol http agar mengupgrade websitenya ke protokol https agar lebih aman dari serangan para *cracker.*

## V. KESIMPULAN

Berdasarkan hasil percobaan penyadapan paket data di jaringan *wifi* Fakultas Teknik UISU, maka dapat diambil kesimpulan bahwa :

1. http://repository.usu.ac.id/password-login adalah link ujicoba *website* berprotokol http, dan dapat di *sniffer* data :
   - *username* : a@gmail.com dan *password* : 12345678
2. https://dashboard.prakerja.go.id/masuk adala link sebagai ujicoba *website* berprotokol https, dan tidak dapat di *sniffer* data *username* dan passwordnya.
3. Dengan mengimplementasikan aplikasi *cain and abel* penulis memberikan kesimpulan bahwa, mengakses *website* dengan protokol http ketika terhubung pada *wifi public* tidak aman bagi data privasi penggunanya.
4. Aplikasi cain and abel dapat menanggkap paket data berupa *username* dan *password* pada *website* http.
5. Aplikasi *cain and abel* tidak dapat menanggkap paket data berupa *username* dan *password* pada *website* https.

## DAFTAR PUSTAKA


[1]. Adzan Abdul Zabar, Fahmi Novianto. 2015, *Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux*". Jurnal Ilmiah Komputer dan Informatika (KOMPUTA) 69 Vol. 4, No. 2, ISSN : 2089-9033.

[2]. https://www.ilmukomputer.org/wp-content/uploads/2007/03/farhan-sniffing.pdf.

[3]. https://www.yuksinau.id/pengertian-wifi/

[4]. https://beon.co.id/news/apa-sih-bedanya-http-dan-https-pelajari-disini

[5]. Pipin, A., 2013, Kamus Teknologi Informasi Komunikasi. Bandung : titan ilmu Bandung.

[6]. Sofana, Iwan, 2010, CCNA *dan Jaringan Komputer*. Bandung: Informatika.

**[7].** Sopandi, Dede, 2008, *Instalasi Dan Konfigurasi Jaringan Komputer*, Penerbit : Informatika, Bandung.