Pemanfaatan *Raspberry Pi* untuk *Hacking* dan *Forensic* dengan metode NIST (*National Institute of Standards and Technology*)

Ilham Taufiqurrohman[1], Nur Widiyasono[2], Husni Mubarok[3]

[1,2,3]*Jurusan Teknik Informatika, Fakultas Teknik, Universitas Siliwangi*

Jalan Siliwangi No.24 Tasikmalaya 46155

[1]ilham.taufiqurrohman@student.unsil.ac.id

[2]nur.w095@gmail.com

[3]husni.mubarok@unsil.ac.id

Abstract - **Cybercrime because of the people who are not responsible, with the aim of damaging, modifying, and eliminating one's data, one of them with hacking techniques to be able to infiltrate into the data storage makes it easy to commit a crime. Treatment can be performed on cybercrime using forensic science as a problem solver. Cybercrime has digital evidence as traces of a criminal case, with digital evidence forensic science analysis to find out what activities performed on a criminal case. This study analyzed digital evidence on the network by utilizing Raspberry pi as a medium for hacking the network and to obtain digital evidence on the network. The method used to perform analysis of digital evidence is NIST (National Institute of Standards and Technology).**

Keywords – **Cybercrime, Digital evidence, Forensic Science, Hacking, NIST (National Institute of Standards and Technology), Raspberry Pi**

I. PENDAHULUAN

Seiring perkembangan teknologi, setiap kebutuhan manusia dapat dibantu dengan menggunakan teknologi untuk menyelesaikan semua aktivitas yang dilakukan. Teknologi yang digunakan oleh manusia memiliki dampak positif dan dampak negatif. Dampak positifnya adalah dapat membantu menyelesaikan aktivitas secara cepat, dan dapat membantu pekerjan yang sulit, dan dampak negatifnya adalah penyalahgunaan dari teknologi itu sendiri yang dilakukan oleh orang-orang yang tidak bertanggungjawab. Maksud dari penyalahgunaan tersebut adalah teknologi digunakan untuk maksud tertentu dengan melakukan tindak kejahatan yang dapat merugikan orang lain. Kejahatan pada teknologi sering disebut *cybercrime. Cybercrime* merupakan istilah dari suatu aktivitas kejahatan dengan komputer atau jaringan sebagai alat, sasaran atau tempat perkara. *Cybercrime* merupakan kejahatan pada komputer. *Cybercrime* memiliki barang bukti yang merupakan jejak dari aktivitas kejahatan yang dilakukan, baik berupa bukti digital ataupun bukti elektronik dan perlu dilakukan penanganan untuk melakukan analisa terhadap barang bukti yang didapatkan dengan pengelolaan menggunakan ilmu forensik. Ilmu forensik yang berhubungam dengan dunia teknologi adalah digital forensik. Salah satu kejahatan yang sering terjadi adalah kejahatan dengan kasus *hacking. Hacking* merupakan satu teknik kejahatan dimana pelaku melakukan pembobolan suatu sistem agar dapat masuk kedalamnya, untuk dapat merusak, mengubah, dan menghapus sistem yang dimiliki orang lain, dengan berbagai maksud dan tujuan yang tidak baik.

Kegiatan yang dilakukan pada *cybercrime* meninggalkan barang bukti, baik itu bukti digital maupun bukti elektronik, bukti digital merupakan salah satu hal yang terpenting dalam sebuah kasus *cybercime* karena semua yang terjadi terekam dan tersimpan pada bukti digital, bukti digital merupakan informasi dalam suatu kasus kejahatan dalam bentuk digital, dan bukti elektronik merupakan bukti berbentuk fisik sebagai media penyimpanan bukti digital ataupun media untuk mendapatkan bukti digital.

Bukti digital dapat dilihat ketika proses kejahatan berlangsung ataupun ketika bukti digital sudah disimpan, bukti digital dapat dilakukan penanganan khusus dengan ilmu digital forensik dengan menggunakan berbagai tools untuk memecahkan dan penarikan kesimpulan dari kasus kejahatan pada bukti digital yang didapatkan.

Berdasarkan permasalahan diatas, maka penelitian yang dilakukan adalah melakukan analisis terhadap bukti digital pada jaringan berbentuk *pcap*, dan bukti elektronik berupa *flashdrive* (*flashdisk*) sebagai media penyimpanan, dengan memanfaatkan *Raspberry pi* dan NIST (*National Institute of Standards and Technology*) sebagai metode analisis bukti digital dengan tahapan analisis.

II. LANDASAN TEORI

A. Digital Forensik

Digital Forensik merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital. Penguasaan ilmu ini tidak hanya ditujukan kepada kemampuan teknis semata tetapi juga terkait dengan bidang lain, seperti bidang hukum [1].

B. Ilmu forensik

Forensik adalah ilmu apa pun yang digunakan untuk tujuan hukum dengan tidak memihak bukti ilmiah untuk digunakan dalam pengadilan hukum, dan dalam penyelidikan dan pengadilan pidana [2].

C. Forensik Jaringan

Forensik Jaringan merupakan ilmu keamanan komputer berkaitan dengan investigasi untuk menemukan sumber serangan pada jaringan berdasarkan bukti log, mengidentifikasi, menganalisis serta merekonstruksi ulang kejadian tersebut. Istilah *Network Forensic* memang di ambil dari terminologi yang berhubungan dengan kriminologi [3].

D. Cybercrime

Cyber Crime adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital [4].

E. Barang bukti

Barang bukti (*Evidence*) yang diartikan pada forensik tidak lain ialah informasi dan data dari apa yang didapatkan pada suatu kasus. Barang bukti adalah bagian terpenting dalam sebuah kasus kejahatan untuk memecahkan kasus tersebut [5].

1) Barang bukti elektronik: Barang bukti ini bersifat fisik dan dapat di kenali secara visual, sehingga investigator dan analis forensik harus sudah memahami serta mengenali masing-masing barang bukti elektronik ini ketika sedang melakukan proses pencarian (*searching*) barang bukti di TKP. Jenis barang bukti elektronik ini antara lain:

- *PC*
- *Notebook*
- *Tablet*
- *Handphone*
- *Flashdisk*
- *Harddisk*
- *CD/DVD*
- *Router,Switch*
- *Kamera*
- *CCTV.*

2) Barang bukti digital: Barang bukti digital sangat rentan terhadap berubahan informasi didalamnya, perlu penanganan untuk menjaga keutuhan barang bukti.

- *Logical File*
- *Deleted File / Unallocated Custer*
- *Lost File*
- *Slack File*
- *Log File*
- *Encrypted File*
- *Steganography File*
- *Office File*
- *Audio File*
- *Image File*
- *Video File*
- *Email / Electronic Mail*
- *User ID and Password*
- *SMS / Short Message Service*
- *Call Log*

F. Password Cracker

Password Cracker adalah program yang mencoba membuka sebuah password yang telah terenkripsi dengan menggunakan sebuah algoritma tertentu dengan cara mencoba semua kemungkinan. Teknik ini sangatlah sederhana, tapi efektivitasnya luar biasa, dan tidak ada satu pun sistem yang aman dari serangan ini, meski teknik ini memakan waktu yang sangat lama, khususnya untuk password yang rumit [6].

Kelas Serangan untuk *cracking password* dibagi menjadi 5 kelas [7], antara lain:

- Kelas A : 10.000 Sandi/detik
  Tipe untuk pemulihan dari *password Microsoft Office* pada Pentium 100.
- Kelas B : 100.000 Sandi / detik
  Tipe untuk pemulihan dari *Windows Password Cache (.pwl Files) password* pada Pentium 100.
- Kelas C : 1.000.000 Sandi / detik
  Tipe untuk pemulihan ZIP atau *password* ARJ pada Pentium 100.
- Kelas D : 10.000.000 Sandi / detik
  Cepat PC, Processor PC Ganda.
- Kelas E : 100.000.000 Sandi / detik
  Workstation, atau kerja beberapa PC secara bersama-sama.
- Kelas F : 1.000.000.000 Sandi / detik
  Tipe untuk skala menengah sampai besar pada komputasi terdistribusi, Superkomputer.

Numerals	0123456789						
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	100	Instant	Instant	Instant	Instant	Instant	Instant
3	1000	Instant	Instant	Instant	Instant	Instant	Instant
4	10,000	Instant	Instant	Instant	Instant	Instant	Instant
5	100,000	10 Secs	Instant	Instant	Instant	Instant	Instant
6	1 Million	1½ Mins	10 Seconds	Instant	Instant	Instant	Instant
7	10 Million	17 Mins	1½ Mins	1½ Mins	Instant	Instant	Instant
8	100 Million	2¾ Hours	17 Mins	1½ Mins	10 Seconds	Instant	Instant
9	1000 Million	28 Hours	2¾ Hours	17 Mins	1½ Mins	10 Seconds	Instant

Gambar 1. Waktu pemecahan *password* dengan karakter angka

Gambar 1 Menjelaskan tentang estimasi waktu yang dibutuhkan untuk memecahkan kombinasi *password* dengan karakter angka saja.

Upper Case Alpha	ABCDEFGHIJKLMNOPQRSTUVWXYZ						
Lower Case Alpha	abcdefghijklmnopqrstuvwxyz						
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	676	Instant	Instant	Instant	Instant	Instant	Instant
3	17,576	< 2 Secs	Instant	Instant	Instant	Instant	Instant
4	456,976	46 Secs	5 Secs	Instant	Instant	Instant	Instant
5	11.8 Million	20 Mins	2 Mins	12 Secs	Instant	Instant	Instant
6	308.9 Million	8½ Hours	51½ Mins	5 Mins	30 Secs	3 Secs	Instant
7	8 Billion	9 Days	22 Hours	2¼ Hours	13 Mins	1¼ Mins	8 Secs
8	200 Billion	242 Days	24 Days	2½ Days	348 Mins	35 Mins	3½ Mins

Gambar 2. Waktu pemecahan *password* dengan karakter huruf (*Uppercase* atau *Lowercase)*

Gambar 2 Menjelaskan tentang estimasi waktu yang dibutuhkan untuk memecahkan kombinasi *password* dengan karakter huruf.

Upper Case Alpha	ABCDEFGHIJKLMNOPQRSTUVWXYZ						
Lower Case Alpha	abcdefghijklmnopqrstuvwxyz						
Numerals	0123456789						
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	1,296	Instant	Instant	Instant	Instant	Instant	Instant
3	46,656	4 Secs	Instant	Instant	Instant	Instant	Instant
4	1.6 million	2½ Mins	16 Seconds	1½ Seconds	Instant	Instant	Instant
5	60.4 million	1½ Hours	10 Mins	1 Min	Instant	Instant	Instant

Gambar 3. Waktu pemecahan *password* dengan karakter angka atau huruf (*Uppercase* atau *Lowercase*)

Gambar 3 Menjelaskan tentang estimasi waktu yang dibutuhkan untuk memecahkan kombinasi *password* dengan karakter angka dan huruf.

Mixed Alpha and Numerals	0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz						
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	3,844	Instant	Instant	Instant	Instant	Instant	Instant
3	238,328	23 Secs	< 3 Secs	Instant	Instant	Instant	Instant
4	15 Million	24½ Mins	2½ Mins	15 Secs	< 2 Secs	Instant	Instant
5	916 Million	1 Day	2½ Hours	15¼ Mins	1½ Mins	9 Secs	Instant
6	57 Billion	66 Days	6½ Days	16 Hours	1½ Hours	9½ Mins	56 Secs
7	3.5 Trillion	11 Years	1 Year	41 Days	4 Days	10 Hours	58 Mins
8	218 Trillion	692 Years	69¼ Years	7 Years	253 Days	25¼ Days	60½ Hours

Gambar 4. Waktu pemecahan *password* dengan gabungan angka dan huruf (*Uppercase* dan *Lowercase*)

Gambar 4 Menjelaskan tentang estimasi waktu yang dibutuhkan untuk memecahkan kombinasi *password* dengan karakter angka dengan huruf besar (*Uppercase*) dan huruf kecil (*Lowercase*).

Mixed Alpha & Symbols	AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz <SP>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~						
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	7,396	Instant	Instant	Instant	Instant	Instant	Instant
8	2.9 Quadrillion	9,488 Years	948 Years	94 Years	57 Years	346 Days	34 Days

Gambar 5. Waktu pemecahan *password* dengan gabungan huruf (*Uppercase* dan *Lowercase*) dan simbol

Gambar 5 Menjelaskan tentang estimasi waktu yang dibutuhkan untuk memecahkan kombinasi *password* dengan karakter huruf dan simbol.

Mixed Alpha, Numerals & Symbols	0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWw					
Password		Class of Attack				
Length	Combinations	Class A	Class B	Class C	Class D	Class E
2	9,216	Instant	Instant	Instant	Instant	Instant
3	884,736	88½ Secs	9 Secs	Instant	Instant	Instant
4	85 Million	2¼ Hours	14 Mins	1½ Mins	8½ Secs	Instant
5	8 Billion	9½ Days	22½ Hours	2¼ Hours	13½ Mins	1¼ Mins
6	782 Billion	2½ Years	90 Days	9 Days	22 Hours	2 Hours
7	75 Trillion	238 Years	24 Years	2½ Years	87 Days	8½ Days
8	7.2 Quadrillion	22,875 Years	2,287 Years	229 Years	23 Years	2¼ Years

Gambar 6. Waktu pemecahan *password* dengan gabungan angka, huruf (*Uppercase* dan *Lowercase*) dan simbol

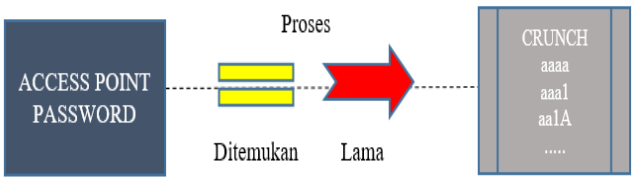
Gambar 6 Menjelaskan tentang estimasi waktu yang dibutuhkan untuk memecahkan kombinasi *password* dengan karakter angka, huruf dan simbol.

1) Bruteforece attack dengan wordlist (kamus kata)

Gambar 7. *Bruteforce attack* dengan *wordlist*

Gambar 7 menjelaskan mengenai *BruteForce Attack* dengan pencocokan menggunakan wordlist merupakan pencocokan dengan daftar kata yang diisi dalam bentuk file teks dengan kemungkinan-kemungkinan kata-kata yang sering digunakan untuk *password* pada *access point*. Hasil pencocokan ini dapat berhasil ditemukan apabila *password* pada *access point* terdapat pada *wordlist*, jika tidak terdapat pada *wordlist* maka *password* tidak ditemukan.

2) Bruteforce attack dengan tools crunch



Gambar 8. *Bruteforce attack* dengan *tools crunch*

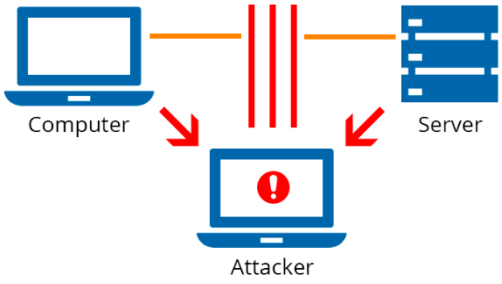
Gambar 8 menjelaskan mengenai *BruteForce Attack* dengan menggunakan *tools Crunch* sebagai pengganti *wordlist* merupakan pencocokan *password* tanpa harus memasukkan kemungkinan-kemungkinan kata-kata dalam bentuk file teks. Hasil pencocokan dengan *tool crunch* pasti dapat ditemukan, namun membutuhkan waktu yang cukup lama untuk mencocokannya apabila kombinasi dari *password access point* panjang dan sulit, karena semua karakter huruf, angka, dan simbol digabungkan dengan berbagai kombinasi.

G. Packet Sniffer

Packet sniffing adalah teknologi yang menangkap paket melewati jaringan di mana ia diinstal. Packet sniffer adalah alat yang memonitor semua data jaringan. Selain itu, dapat mencegat dan log lalu lintas masuk dan keluar di seluruh jaringan [8].

H. Man In The Middle Attack (MITM Attack)

Penyerangan dengan teknik *man-in-the-middle (disingkat MITM)* adalah sebuah bentuk penyadapan dimana sang penyerang membuat sebuah koneksi yang independen antara korban dan mengirimkan pesan diantara para korban yang mengira mereka sedang berkomunikasi pada sebuah koneksi privat dimana sebenarnya semua percakapan tersebut diatur oleh sang penyerang. Metode ini, sang penyerang diharuskan untuk bisa menyadap semua pesan yang dikomunikasikan antara kedua korban dan memasukkan pesan baru. Penyerangan ini hanya bisa sukses jika dan hanya jika sang penyerang bisa menyamar menjadi setiap endpoint dari korban dengan persetujuan yang lainnya [9].



Gambar 9. Teknik *MITM Attack*

Gambar 9 merupakan skema dari teknik MITM (*Man In The Middle*) *Attack*. Jalur data dari *computer client* lain yang terhubung ke *server* akan diputuskan dan dialihkan terlebih dahulu ke *computer attacker*, sehingga data yang diakses dari *computer cilent* ke *server*, melewati terlebih dahulu ke *computer attacker* agar data dapat diambil oleh *attacker*.

I. Raspberry Pi

Raspberry Pi adalah komputer berukuran kartu kredit yang dikembangkan di Inggris oleh Yayasan Raspberry Pi [10].

Gambar 10. *Raspberry Pi 2*

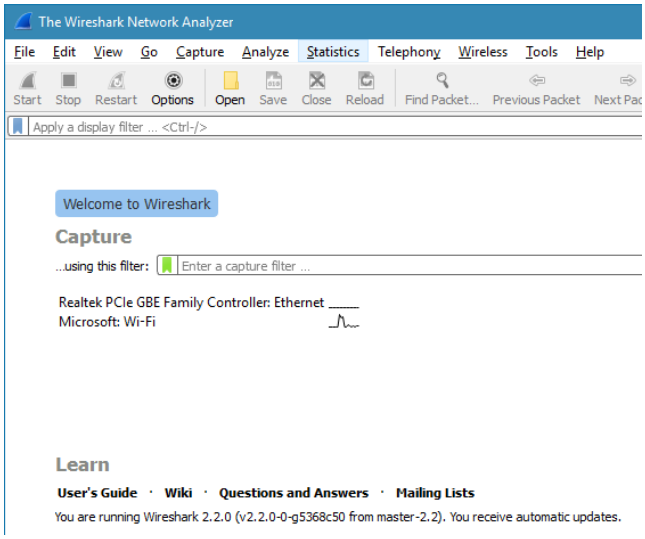
Gambar 10 merupakan bentuk fisik dari *Raspberry Pi* 2, yang telah dilengkapi *port USB , LAN port , audio jack, HDMI port, MicroSD card,* serta *pin-pin* untuk menghubungkan dengan komponen lain seperti *button, dan LED.*

J. Wireshark

Wireshark memungkinkan pengguna mengamati data dari jaringan yang sedang beroperasi atau dari data yang ada di disk, dan langsung melihat dan menyusun data yang tertangkap. Informasi singkat dan datail bagi masing-masing paket, termasuk full header dan porsi data, bisa diperoleh. Wireshark mempunyai beberapa fitur termasuk display filter

e-ISSN : 2443-2229

language yang kaya dan kemampuan untuk merekonstruksi kembali sebuah aliran pada sesi TCP [11].



Gambar 11. *Wireshark*

Gambar 11 menjelaskan tampilan dari halaman utama *Wireshark*, dan terdapat daftar *adapter network* yang terhubung ke perangkat (*computer*).

K. PCAP File

PCAP file merupakan singkatan dari *Packet capture*, *pcap* merupakan file yang didapatkan dari tools sniffing seperti *wireshark*, *ettercap* maupun tools lain yang bertujuan untuk mengetahui isi dari aktivitas jaringan internet. *Packet Capture* juga merupakan suatu teknik atau metode untuk meng-capture suatu paket data yang melewati suatu jaringan komputer. Metode *Packet Capture* ini biasanya digunakan dalam tools keamanan jaringan untuk menganalisa traffic jaringan. Hampir semua paket data dapat di-capture oleh metode tersebut, bahkan sampai paket-paket yang sangat detail sekalipun di-capture oleh metode ini. Paket-paket yang telah tertangkap pun sulit untuk dimengerti oleh orang yang akan mempelajari *Packet Capture* [12].

L. Kali Linux RPi

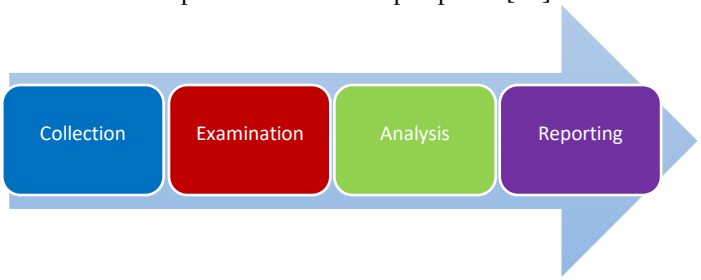
Sistem operasi yang digunakan pada penelitian ini menggunakan *Kali Linux RPi.*

Gambar 12. Kali Linux Rpi

Gambar 12 merupakan logo dari Sistem Operasi *Kali Linux Rpi*. *Kali Linux Rpi* merupakan sistem operasi untuk tujuan digital forensik dengan pengujian penetrasi yang digunakan pada mikrokontroler seperti Raspberry Pi. Kali linux Rpi merupakan distribusi dari keluarga debian, dengan Sistem Operasi versi 2016.1, Kernel versi 4.1.19-v7, dan arsitektur ARMv71.

M. NIST

Metode yang digunakan untuk melakukan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan metode NIST (*National Institute of Standards Technology*). Transformasi pertama terjadi saat data yang dikumpulkan diperiksa, lalu mengekstrak data dari Media dan mengubahnya menjadi format yang bisa diproses oleh alat forensik. Kedua, data ditransformasikan menjadi informasi melalui analisis. Akhirnya, transformasi informasi menjadi bukti analogi dengan mentransfer pengetahuan ke dalam tindakan menggunakan informasi yang dihasilkan oleh analisis dalam satu atau beberapa cara selama fase pelaporan [13].



Gambar 13. Tahapan Metode NIST (*National Institute of Standars Technology*)

Gambar 13 merupakan gambaran skema dari metode NIST *(National Institute of Standars Technology)* sebagai tahapan untuk analisis bukti digital dan bagian dari tahapan penelitian, dengan tahapan yaitu *collection*, *examination*, *analisys*, *reporting*.

III. METODOLOGI

A. *Tahapan Penelitian*

Merupakan langkah-langkah dalam melakukan penelitian, berikut tahapan penelitian yang dilakukan sebagai berikut:

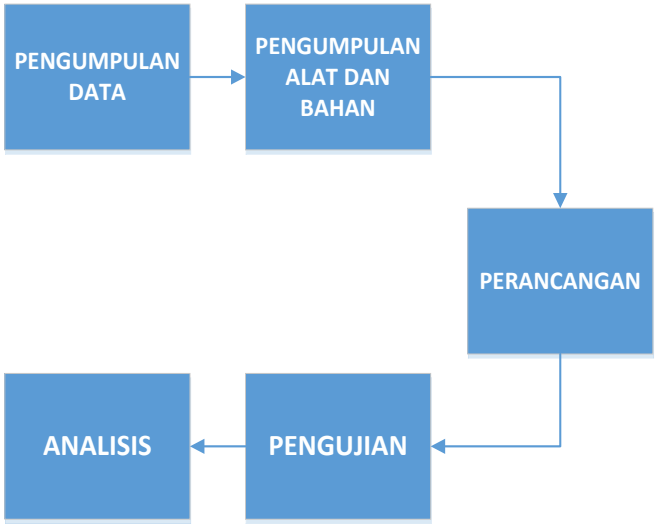
1) Pengumpulan data: Pengumpulan informasi dari sumber yang berkaitan dengan penelitian, studi literatur yaitu sumber-sumber dari jurnal, buku, internet, artikel, dan lain-lain.

2) Pengumpulan alat dan bahan: Pengumpulan kebutuhan-kebutuhan yang digunakan pada penelitian, baik berupa perangkat keras, dan perangkat lunak yang mendukung dalam pembuatan alat.

3) Perancangan: Membuat rancangan dan konfigurasi pada perangkat keras, perangkat lunak untuk membangun sistem dari alat.

4) Pengujian: Pengujian sistem dari alat yang sudah dilakukan, dan proses mendapatkan bukti digital.

5) Analisis: Proses untuk melakukan analisis terhadap bukti digital yang telah didapatkan.



Gambar 14. Tahapan Penelitian

Gambar 14 merupakan tahapan dari penelitian yang dilakukan untuk membuat suatu sistem atau alat dan memperoleh bukti digital dengan alat tersebut sehingga bukti digital tersebut dapat lakukan analisis untuk mengetahui informasi di dalamnya, dengan tahapan pengumpulan data, pengumpulan alat dan bahan, perancangan, pengujian, dan analisis.

B. *Kebutuhan bahan*

1) Perangkat Keras

Beberapa perangkat keras yang dibutuhkan untuk memenuhi pembuatan alat, berikut dijelaskan pada Tabel I.

TABEL I
PERANGKAT KERAS YANG DIBUTUHKAN

NO	NAMA	JUMLAH
1	Raspberry Pi 2	1 Unit
2	MicroSD 16 GB	1 Unit
3	Wireless Adapter TP Link WN722N	1 Unit
4	Flashdisk	1 Unit
6	LED	4 Unit
7	Pushbutton	4 Unit
8	Resistor 330 Ohm	4 Unit
9	Kabel jumper	16 Buah
10	Box	1 Unit

2) Perangkat lunak

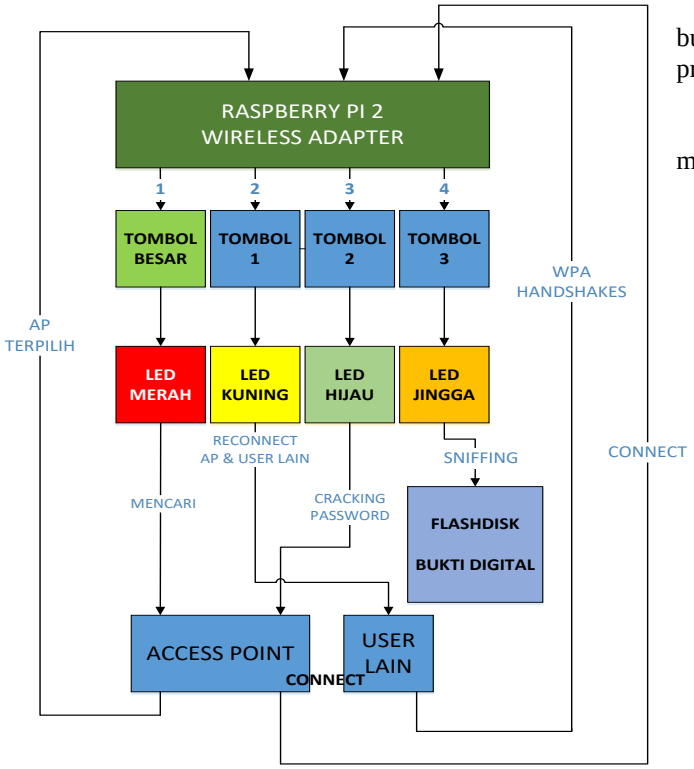
Beberapa perangkat lunak yang dibutuhkan untuk memenuhi membangun sistem pada alat, berikut dijelaskan pada Tabel II.

TABEL II
PERANGKAT LUNAK YANG DIBUTUHKAN

NO	NAMA	FUNGSI
1	Kali Linux RPi	Sistem Operasi
2	Bash Script	Program Sistem
3	Python	Program pengontrol perangkat keras
4	Aircrack-ng	Tool hacking / cracking password
5	Ettercap	Tool sniffing / untuk mendapatkan bukti digital
6	Wireshark	Tool untuk proses analisis bukti digital

C. *Perancangan*

1) Perancangan Sistem: Tahapan pembuatan rancangan dari sistem secara keseluruhan.



Gambar 15. Diagram blok sistem

Gambar 15 merupakan skema proses dari sistem pada alat yang dibuat untuk mendapatkan bukti digital (*pcap*) dari jaringan yang dimulai dari *Raspberry Pi 2*, diatur dengan tombol-tombol dengan berbagai proses hingga bukti digital (*pcap*) tersimpan di bukti elektronik yaitu *flashdisk.*

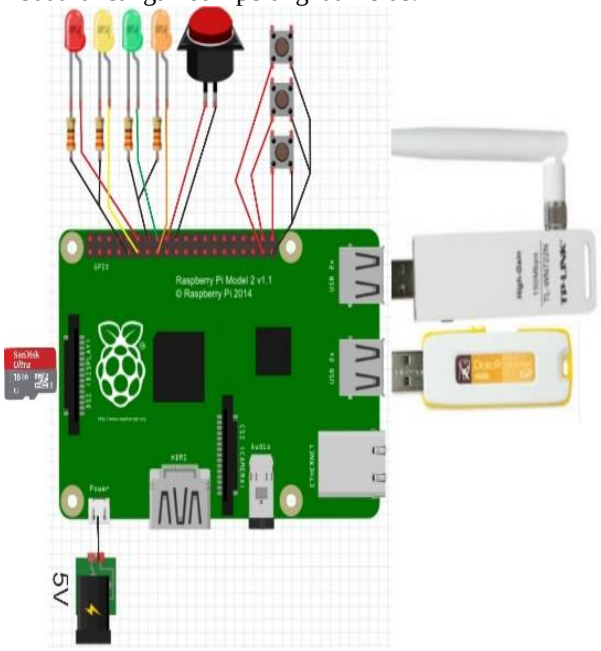
Untuk mendapatkan bukti digital pada sistem yang dibuat diperlukan syarat sebagai berikut yaitu adanya *access point*, adanya *user* lain yang terhubung ke *access point* yang sama, terjadi *WPA Handshakes* untuk mendapatkan enkripsi dari password, proses *cracking password* dilakukan, *password* ditemukan, proses *sniffing* dilakukan, dan bukti digital didapatkan, berikut dijelaskan pada Tabel III.

TABEL III
KEMUNGKINAN PADA SISTEM

Kemungkinan	*Access point*	*User* lain	*WPA Handshakes*	*Cracking*	*Password*	*Sniffing*	Bukti digital *(PCAP)*
1	-	-	-	-	-	-	-
2	√	-	-	-	-	-	-
3	√	√	-	-	-	-	-
4	√	√	√	√	-	-	-
5	√	√	√	√	√	√	√

Penjelasan dari Tabel III bahwa, untuk mendapatkan bukti digital semua tahap harus terlewati sampai semua proses berhasil dilakukan (kemungkinan pada point 5).

2) Perancangan perangkat keras: Tahapan untuk membuat rancangan dari perangkat keras.



Gambar 16. Rancangan perangkat keras

Gambar 16 adalah skema rancangan dari alat yang dibuat terdiri dari *microSD*, *LED* disertai *resistor* 330 Ohm, tombol-tombol, *wireless adapter*, *flashdisk*, dan catu daya dengan arus 5V.

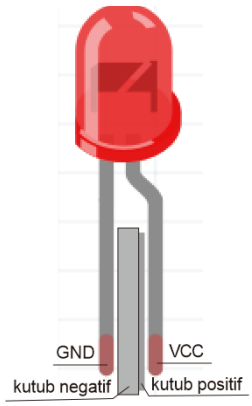
3) Perancangan perangkat lunak: Tahapan untuk melakukan pengaturan dari sistem dan pemrograman. Pengaturan pada perangkat lunak dikendalikan dengan aplikasi SSH (Secure Shell) atau RDP (*remote desktop protocol*) yang berfungsi untuk mengendalikan *raspberry pi* dengan satu jaringan yang sama dengan *LAN cable*.

- Instalasi sistem operasi kali linux RPi pada microSD.
- *Update* dan *upgrade kali linux repositories.*
- Instalasi modul atau *library program* yang mendukung seperti *pip-python*, *pip-wireless*, *RPi.GPIO*.
- Pembuatan program atau *coding*.

IV. HASIL DAN PEMBAHASAN

A. Pengujian

1) Pengujian LED: Pengujian LED tanpa terhubung atau masih terpisah dengan sistem dengan menguji menggunakan baterai kancing yang dihubungkan ke kaki-kaki pada LED, digambarkan pada gambar 17.



Gambar 17. Pengujian LED

2) Pengujian LED dengan koding: Menguji bekerja atau tidaknya LED dengan menggunakan koding *python programming*.

```
import RPi.GPIO as GPIO
import time
GPIO.setmode(GPIO.BCM)
GPIO.setwarnings(False)
GPIO.setup(18,GPIO.OUT)
GPIO.output(18,GPIO.HIGH)
```

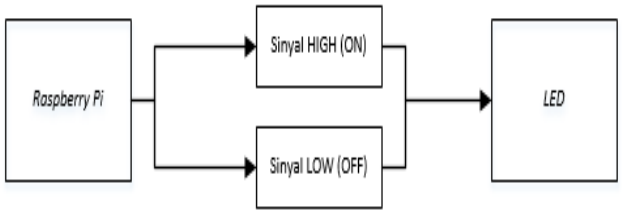
Listing 1. Koding untuk menyalakan LED

Listing 1 menjelaskan koding (bahasa *python*) yang dibuat untuk menyalakan LED , yang terhubung ke *Raspberry Pi* di PIN 18 dengan perintah kunci *GPIO.output (**18**,GPIO.**HIGH**)*.

```
import RPi.GPIO as GPIO
import time
GPIO.setmode(GPIO.BCM)
GPIO.setwarnings(False)
GPIO.setup(18,GPIO.OUT)
GPIO.output(18,GPIO.LOW)
```

Listing 2. Koding untuk mematikan LED

Listing 2 menjelaskan koding (bahasa *python*) yang dibuat untuk mematikan *LED* , yang terhubung ke *Raspberry Pi* di PIN 18 dengan perintah kunci *GPIO.output (**18**,GPIO.**LOW**)*.



Gambar 18. Diagram blok LED dengan program

Gambar 18 menjelaskan skema jika *Raspberry Pi* memberikan sinyal terhadap *LED* untuk proses menyalakan dan mematikan.

Untuk melihat hasil dari pengujian *LED* yang dikendalikan koding *python* untuk tiap masing-masing *LED*, dijelaskan pada tabel IV.

TABEL IV
HASIL PENGUJIAN LED DENGAN KODING

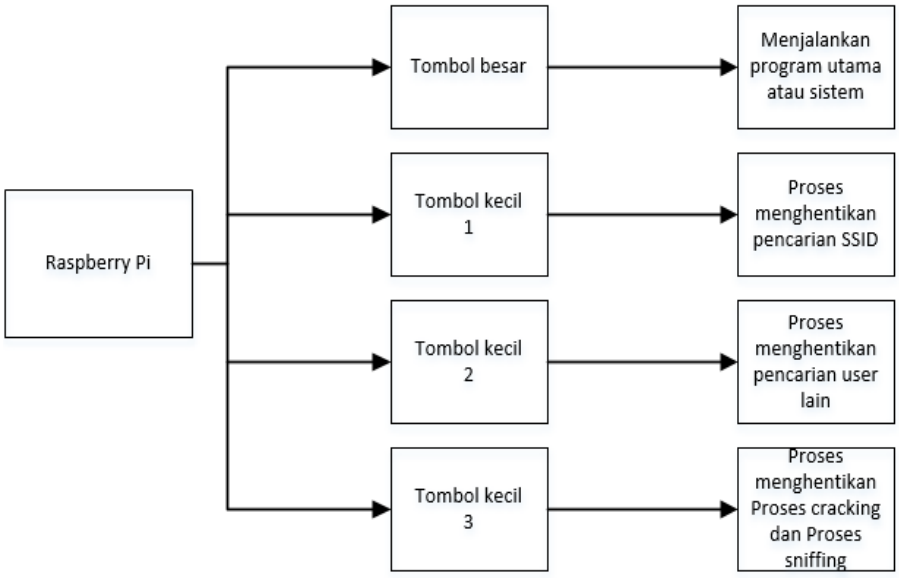
LED	PIN	*ON*		*OFF*	
		Harapan	**Hasil**	**Harapan**	**Hasil**
Merah	18	Menyala	Menyala	Mati	Mati
Kuning	17	Menyala	Menyala	Mati	Mati
Hijau	23	Menyala	Menyala	Mati	Mati
Jingga	22	Menyala	Menyala	Mati	Mati

3) Pengujian pushbutton dengan koding: Menguji bekerja atau tidaknya p*ushbutton* dengan menggunakan koding *python programming*.

```
#!/bin/python
import RPi.GPIO as GPIO
import time
import os
GPIO.setmode(GPIO.BCM)
GPIO.setup(24, GPIO.IN, pull_up_down =
GPIO.PUD_UP)
def Shutdown(channel):
    os.system("python red.py")
GPIO.add_event_detect(24,
GPIO.FALLING, callback = Shutdown,
bouncetime = 2000)
while 1:
    time.sleep(1)
```

Listing 3. Koding *pushbutton* untuk menyalakan LED

Listing 3 menjelaskan koding yang dibuat untuk menyalakan *LED* dengan menggunakan *pushbutton* (tombol), yang terhubung ke *Raspberry Pi* dengan memanggil bahasa python yang dibuat sebelumnya yaitu seperti pada listing 1 dengan perintah kunci *os.system ("**python red.py**")*.



Gambar 19. Diagram blok *pushbutton* dengan koding

Gambar 19 menjelaskan skema jika *Raspberry Pi* memberikan sinyal terhadap *pushbutton* (tombol) untuk melakukan proses terhadap sistem pada alat.

Untuk melihat hasil dari pengujian *pushbutton* (tombol) yang dikendalikan koding *python* untuk tiap masing-masing *pushbutton* (tombol), dijelaskan pada tabel V.

TABEL V
HASIL PENGUJIAN *PUSHBUTTON* DENGAN KODING

Pushbutton	**PIN**	**Fungsi**	**Harapan**	**Hasil**
Pushbutton besar	24	Pencarian SSID	Berfungsi	Berfungsi
Pushbutton kecil 1	21	Pencarian user lain yang terhubung ke SSID yang sama	Berfungsi	Berfungsi
Pushbutton kecil 2	20	Proses Cracking	Berfungsi	Berfungsi
Pushbutton kecil 3	26	Proses Sniffing	Berfungsi	Berfungsi

4) Pengujian sistem: Menguji keberhasilan komponen dan sistem yang telah dibangun dan dirancang sehingga menjadi suatu alat.

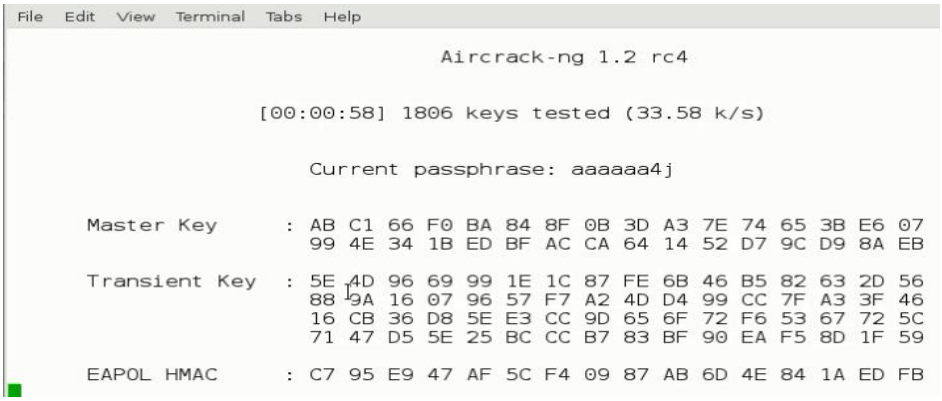
- Ketik *python bigbutton.py* pada terminal, proses pencarian SSID setelah menekan *pushbutton* besar dan pemilihan *user* lain yang terhubung ke SSID yang sama menekan *pushbutton* kecil 1.

```
CH  1 ][ Elapsed: 24 s ][ 2016-10-10 08:30 ][ WPA handshake: 18:44:E6:CA:BA:08

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

18:44:E6:CA:BA:08  -49 100      254      252    3   1  54e  WPA2 TKIP   PSK  Wakwe

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

18:44:E6:CA:BA:08  DC:85:DE:79:E9:A0  -24   54e-54e     0       185
18:44:E6:CA:BA:08  12:34:56:C2:B1:E0  -33    1e- 1      0       111
```

Gambar 20. Terjadi *WPA handshake*

Gambar 20 merupakan tampilan proses terjadinya *WPA handshake* setelah memilih SSID dan user lain yang terhubung ke SSID yang sama.

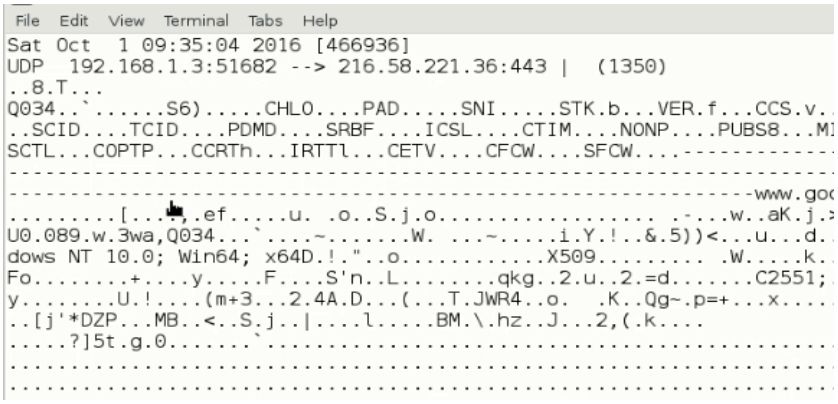
- Proses *cracking password* setelah menekan *pushbutton* kecil 2.



Gambar 21. Proses *cracking*

Gambar 21 merupakan tampilan dari proses *cracking password* dari SSID yang terhubung dengan *Raspberry Pi 2* setelah menekan *pushbutton* (tombol) kecil 2.

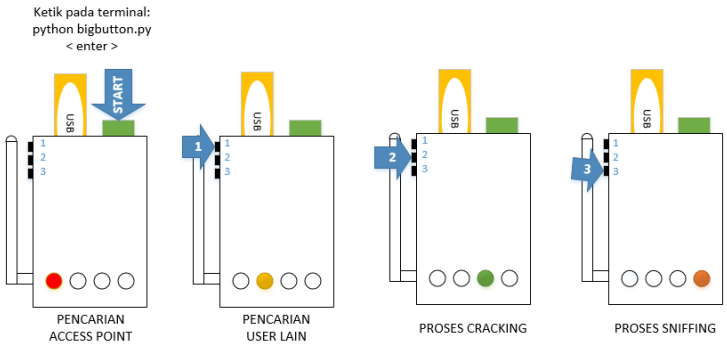
- Proses *sniffing* setelah menekan *pushbutton* kecil 3.



Gambar 22. Proses *sniffing*

Gambar 22 merupakan tampilan dari proses *sniffing* dari komputer *client* yang sedang melakukan akses ke sebuah *server*.

- Pengujian di sisi perangkat lunak
  Proses pengujian dan penggunaan alat jika dilihat dari sisi perangkat keras.

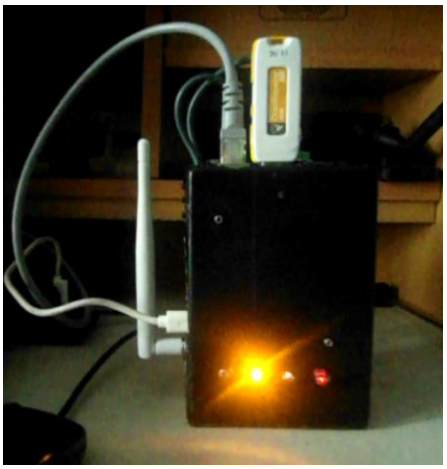


Gambar 23. Pengujian dari sisi perangkat keras

Gambar 23 merupakan tahapan penggunaan alat jika dilihat dari perangkat keras, dengan proses yaitu mengetikan ***python bigbutton.py*** pada terminal untuk mengaktifkan dan menjalankan sistem, kemudian tekan tombol hijau yang besar untuk proses pencarian SSID (*access point*) maka indikator LED merah menyala, kemudian setelah daftar SSID muncul maka proses pencarian dapat dihentikan dengan menekan tombol kecil 1 yaitu melanjutkan ke proses pencarian user yang terhubung ke access point yang sama (yang terpilih sesuai kekuatan *access point*) dengan indikator LED merah mati dan LED kuning menyala, setelah muncul daftar user yang terhubung ke acceee point yang sama dan muncul *WPA Handshakes* pada layar maka proses dapat dihentikan untuk melanjutkan ke proses *cracking password* dengan menekan tombol kecil 2 dengan indikator LED kuning mati dan LED hijau menyala, jika *password* dari *access point* sudah ditemukan maka selanjutnya proses menghubungkan *raspberry pi* dengan *access point* ,kemudian melanjutkan ke prosess *sniffing* dengan menekan tombol kecil 3 dengan indikator LED hijau mati dan LED jingga menyala, jika proses *sniffing* ingin dihentikan maka selanjutnya menekan tombol kecil 3 sekali lagi, maka semua proses sudah dihentikan dan *file pcap* secara otomatis sudah tersimpan ke *USB flash* (*flashdisk*).

Gambar 24. Alat sedang proses pencarian SSID (*Access point*)

Gambar 24 adalah tampilan dari sisi perangkat keras dengan LED merah menyala bahwa proses pencarian SSID sedang berlangsung.



Gambar 25. Alat sedang melakukan proses *WPA Handshakes*

Gambar 25 adalah tampilan dari sisi perangkat keras dengan LED kuning menyala bahwa proses *WPA Handshake* (mendapatkan enkripsi dari *client* lain terhadap SSID yang sama) sedang berlangsung.

Gambar 26. Alat sedang melakukan proses *cracking password*

Gambar 26 adalah tampilan dari sisi perangkat keras dengan LED hijau menyala bahwa proses *cracking password* SSID sedang berlangsung.

Gambar 27. Alat sedang melakukan proses *sniffng*

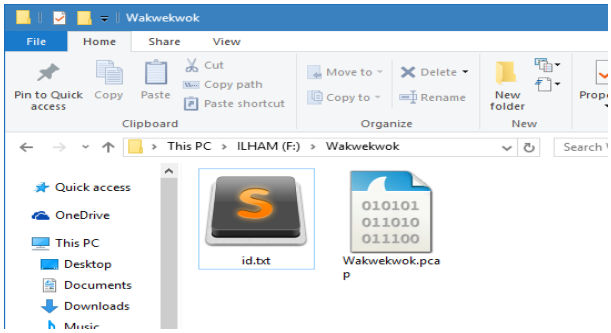
Gambar 27 adalah tampilan dari sisi perangkat keras dengan LED jingga menyala bahwa proses sniffing sedang berlangsung.

Untuk melihat hasil dari pengujian alat, berikut beberapa pengujian percobaan yang telah dilakukan, dijelaskan pada Tabel VI.

TABEL VI
HASIL PENGUJIAN SISTEM

Pengujian	Access Point	User lain	WPA Handshakes	Cracking	Sniffing	Bukti digital
1	Wakwekwok	√	√	√	√	√
2	NUABi	√	-	-	-	-
3	HANAWA	√	√	√	√	√
4	MyPublicWiFi	√	√	√	√	√

- Mendapatkan bukti digital
  Proses *sniffing* dari alat menghasilkan bukti digital pada jaringan.



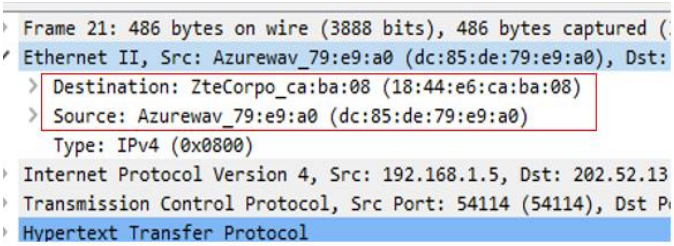
Gambar 28. Bukti digital yang didapatkan

Gambar 28 merupakan contoh bukti digital yang didapatkan dari alat yang telah dibuat, berupa *file pcap.*

B. *Analisis*

Merupakan tahap melakukan analisis pada bukti digital yang didapatkan.

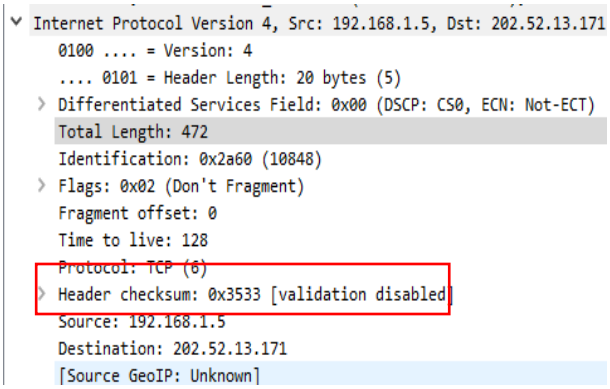
1) Analisis bukti digital pada *data link*



Gambar 29. Analisis pada *data link*

Gambar 29 adalah tampilan dari isi bukti digital menggunakan wireshark, dengan data yang dilihat pada *data link* di frame 21 yang berisi *MAC Address* perangkat yang digunakan oleh *client* lain yang terhubung ke SSID yang sama dan *MAC Address* dari perangkat yang digunakan oleh *server web* yang diakses oleh *client* lain tersebut.

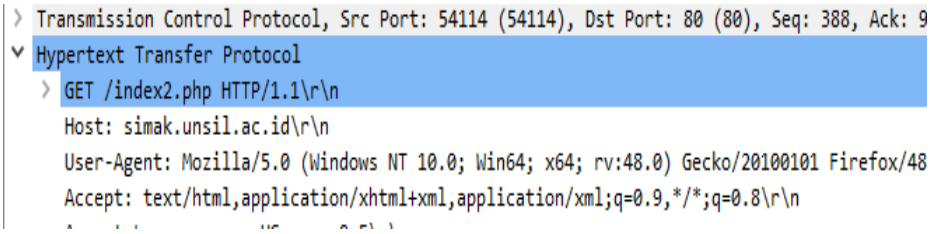
2) Analisis bukti digital pada *network layer*



Gambar 30. Analisis pada network layer

Gambar 30 adalah tampilan dari isi bukti digital menggunakan wireshark, dengan data yang dilihat pada *network link* di frame 21 yang berisi *IP Address* perangkat yang digunakan oleh *client* lain yang terhubung ke SSID yang sama dan *IP Address* dari perangkat yang digunakan oleh *server web* yang diakses oleh *client* lain tersebut.

3) Analisis bukti digital pada *HTTP detail*



Gambar 31. Analisis pada *HTTP detail*

Gambar 31 adalah tampilan dari isi bukti digital menggunakan wireshark, dengan data yang dilihat pada *HTTP detail* di frame 21 yang berisi *browser, sistem operasi, website* yang diakses, serta *file* atau *link* dari *website* yang diakses (*index2.php*) oleh client lain tersebut.

C. Reporting

Frame No. 21			
Waktu	Sep 3, 2016 00:02:52.947028000 SE Asia Standard Time		
Panjang Frame	Frame Length: 486 bytes (3888 bits)		
Protokol	eth:ethertype:ip:tcp:http:data		HTTP
Source MAC	dc:85:de:79:e9:a0	**Destination MAC**	18:44:e6:ca:ba:08
Source IP	192.168.1.5	**Destination IP**	202.52.13.171
Source Port	541114	**Destination Port**	80
Host	simak.unsil.ac.id		
Jenis Info	GET /index2.php HTTP/1.1		
Browser	Firefox/48.0		
Sistem Operasi	Windows NT 10.0; Win64; x64		
Kesimpulan	**Frame No.3,** Protokol paket data yang digunakan adalah **HTTP** (*Hypertext Transfer Protocol*) yaitu protokol yang digunakan untuk mentransfer data melalui web. Ini adalah bagian dari protokol Internet dan mendefinisikan perintah dan jasa yang digunakan untuk transmisi data sebuah halaman web. Data lewat pada Sabtu, 3 September 2016, 00.02.52, oleh pengguna dengan **IP Address** 192.168.1.5 dan **MAC Address** dc:85:de:79:e9:a0 menggunakan port 54114 kepada **IP Address** 202.52.13.171 dan **MAC Address** 18:44:e6:ca:ba:08 dengan port 80 mengakses simak.unsil.ac.id informasi pada file index2.php, melakukan akses dengan browser firefox v48 dan sistem operasi Windows 10 64bit.		

Gambar 32 Contoh *report* atau laporan dari frame 21 pada *wakwekwok.pca*

Gambar 32 merupakan contoh *report* atau laporan dari bukti digital yang didapatkan tadi dengan contoh pada *frame* 21, yang telah dilihat informasinya pada proses analisis.

D. Kelebihan dan Kekurangan

1) *Kelebihan:* Alat yang dibuat membantu mendapatkan *file pcap* berisi aktivitas pada jaringan.
2) *Kekurangan:*
   - Program yang dibuat belum dapat dijalankan secara otomatis ketika alat dinyalakan, dan diperlukan aplikasi untuk mengatur *autorunning.*
   - *Access point* belum dapat dipilih sesuai keinginan, karena sistem yang dibuat memilih access point dilihat dari kekuatan sinyal access point yang ada pada *tools aircrack-ng*.
   - Waktu untuk memecahkan *password* belum cepat terhadap *password* yang rumit dan panjang, karena menggunakan teknik *brute-force attack.*

IV. KESIMPULAN

Alat yang dirancang sudah dapat digunakan untuk mendaatkan bukti digital atau file berekstensi *pcap*, dengan tahapan pencarian *access point*, terjadi *WPA Handshakes*, *cracking password* , *password* ditemukan, terhubung ke *access point*, *sniffing*, *file pcap* didapatkan.

DAFTAR PUSTAKA

[1] B. Raharjo, "SEKILAS MENGENAI FORENSIK DIGITAL," *Jurnal Sosioteknologi*, 2013.
[2] E. S. Wijaya and Y. P. , "Integrasi Metode Steganografi DCS pada Image dengan Kriptografi Blowfish sebagai Model Anti Forensik untuk Keamanan Ganda Konten Digital," 2015.
[3] R. U. Putri and J. E. Istiyanto, "Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada," 2012.
[4] M. N. Al-Azhar, Digital Forensic : Panduan Praktis Investigasi Komputer, Jakarta: Salemba Infotek, 2012.
[5] K. E. Pramudita, "Brute Force Attack dan Penerapannya pada Password Cracking," p. 1, 2010.
[6] I. Lucas, "Password Recovery Speeds," 2009. [Online]. Tersedia:http://www.lockdown.co.uk/?pg=combi&s=articles.
[7] D. C. Gandhi, G. Suri, R. P. Golyan, P. Saxena and B. K. Saxena, "Packet Sniffer – A Comparative Study," *International*, p. 1, 2014.
[8] K. Ramadhan, "Pengujian Man-in-the-middle Attack Skala Kecil dengan Poisoning," p. 2, 2011.
[9] R. Flickenger, Jaringan Wireless di Dunia Berkembang, wndw.net, 2007.
[10] F. P. Chandradiva, "Perancangan dan Implementasi Program Aplikasi Capture Dan Identifikasi Paket Pada Wireless Lan Berbasis Linux," 2013.
[11] E. Rachman, F. Candrasyah and F. D. Sutera, RaspberryPi : Mikrokontroler Mungil yang Serba Bisa, Yogyakarta : Andi Publisher , 2014.
[12] A. Tahir, Penegakan Hukum Cybercrime di Indonesia, Yogyakarta: Pascasarjana Universitas Gajah Mada, 2009.
[13] K. Kent, S. Chevalier, T. Grance and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, Gaithersburg: NIST, 2006.