Analysis Of WPA2 Security Test At PT. Andaglos Global Teknologi Using Fluxion

Dwi Nanda Widiatama[1], Rionaldi Ali[2]
[1,2]Departement of Informatics Engineering, IIB Darmajaya,
Jl. Z.A Pagar Alam No. 93 Lampung, Indonesia
Email: nandasangpetani@gmail.com, rionaldi@darmajaya.ac.id

ABSTRACT
PT. Andaglos Global Technology uses internet service providers and is equipped with wifi facilities. The location of the office is in the terminal and is adjacent to the shop and other buildings. This resulted in the wifi network at PT. Andaglos Global Technology is often exploited by illegal users around the office, so that the impact on the internet speed decreases. Even the employees of PT. Andaglos Global Teknologi claimed to have been a victim of hacking in its social media after accessing the network at PT. Andaglos Global Technology. To solve this problem, penetration testing is done using FLUXION on PT. Andaglos Global Technology with the method (Action Research) which consists of several stages, namely Diagnosing, Action Planing, Action Taking, Evaluating and Specifyng Learning, to determine the level of security on the network of PT. Andaglos Global Technology. Penetration testing with FLUXION proves that network security at PT. Andaglos Global Technology works well in securing passwords, but FLUXION is able to get passwords from these networks, not by breaking into security but by deceiving network users by creating the same login form as the routers used by PT. Andaglos Global Technology, so that unknowingly network users have given the password to the fake login page, which resulted in the network being accessed by users illegally.

Keywords: Wireless Network Penetration Testing, Fluxion

1. INTRODUCTION

1.1 Background.

PT. Andaglos Global Teknologi (PT. AGT) is a startup company engaged in the field of manufacturing applications and software. The safety factor is still not a priority for PT. AGT. The office location of PT. AGT is located in a dense building area, so WiFi networks have the possibility to be used by users outside of PT. AGT. In fact, one of the employees of PT. AGT was once a victim of hacking after he used the WiFi network of PT. AGT to access social media services.

1.2 Research Objectives.

1. Running a series of tests on the PT. AGT network so that recommendations or solutions can be produced that can be applied to the PT. AGT network.
2. Developing Fluxion with the addition of Indonesian and adding web interface to the Fluxion directory.

2. LITERATURE REVIEW

2.1 Network Security.

At present Wi-Fi facilities for the public are the main target in cyber crime, therefore we should not underestimate a network's security.

Recently, hacker forums in cyberspace are rife with discussions about a program that is said to be able to get wireless passwords of WPA2 security type without having to crack the algorithm used.

2.2 Network Attacks.

1. Packet Sniffer.
   Is a data theft technique that is done by monitoring or analyzing data packets that are transmitted from the client computer to the server. The tools commonly used for packet sniffing are usually Wireshark and Netcut. This packet sniffing is usually done by hackers or dangerous intruders to carry out prohibited actions such as stealing passwords, and retrieving other important data.

2. ARP Spoofing.
   Is a technique of attacking on a local computer network with either wired or wireless media, which allows an attacker to sniff out data frames on a local network and / or modify traffic or even stop traffic. ARP spoofing is a concept of tapping attacks between two machines that are communicating or called MITM (Man in the Middle Attack). The principle of ARP spoofing attacks exploits weaknesses in the computer network technology itself that uses ARP broadcast.

3. Brute Force Attack.
   Is a method for hacking passwords (password breaking) by trying all possible random combinations that exist or that exist in the "wordlist". This method will successfully find the password you want to hack. However, the process for hacking passwords using this method will take a lot of time.

2.3 Fluxion.

Fluxion is a security audit and social engineering research tool. This is a development of the linset by vk496 in the hope that it will be even better with fewer bugs and more functions.

```
            FLUX 0.24 (rev.  123) by  deltax
      Page: https://github.com/deltaxflux/fluxion
                    Latest rev. [/]
```

Figure 1. Fluxion.

2.4 Kali Linux.

Linux is an operating system, just like Windows. Linux is an open source operating system, meaning that linux can be seen as its source code, modified, and developed by anyone.

3. METHOD

3.1 Data Collecting.

a. Observation.

Systematic observation and recording of objects to be examined, observations made by researchers by means of observation and recording of providers used, routers used. and WiFi signal radius.

b. Interview.

Direct interviews were conducted at the leaders of PT. AGT to get information about the WiFi network they have.

3.2 Penetration Testing Method.

In this research the penetration testing method uses the Action Research method. The stages of this action research are diagnosing, action planning, action taking, evaluating, specifying learning.

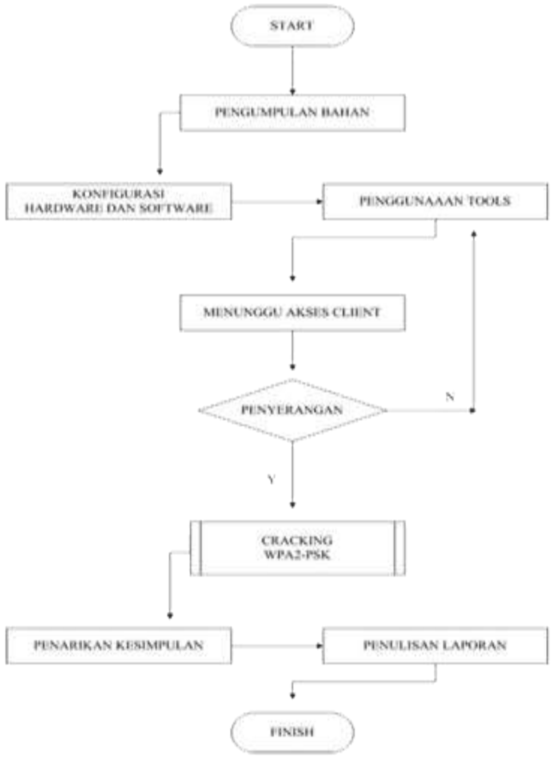


Figure 2. Action Research Flowchart.

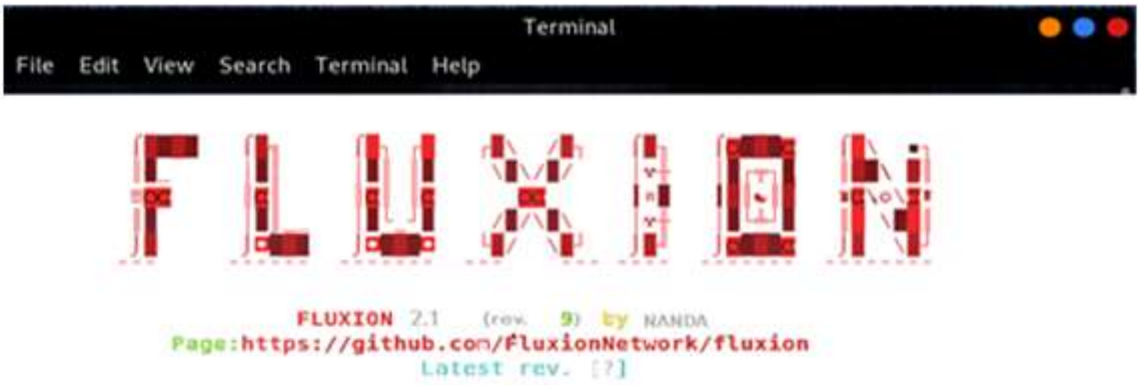
3.3 Software Requirements.

To run penetration testing in this study we use software such as: Kali Linux, Fluxion, DHCP, HOSTAPD, MDK3, LIGHTTPD. Medium hardware that we use is: a minimum of Intel Core i3 processor, a minimum of 2GB of memory, a minimum of 2GB of graphics memory.

4. RESULT AND DISCUSSION

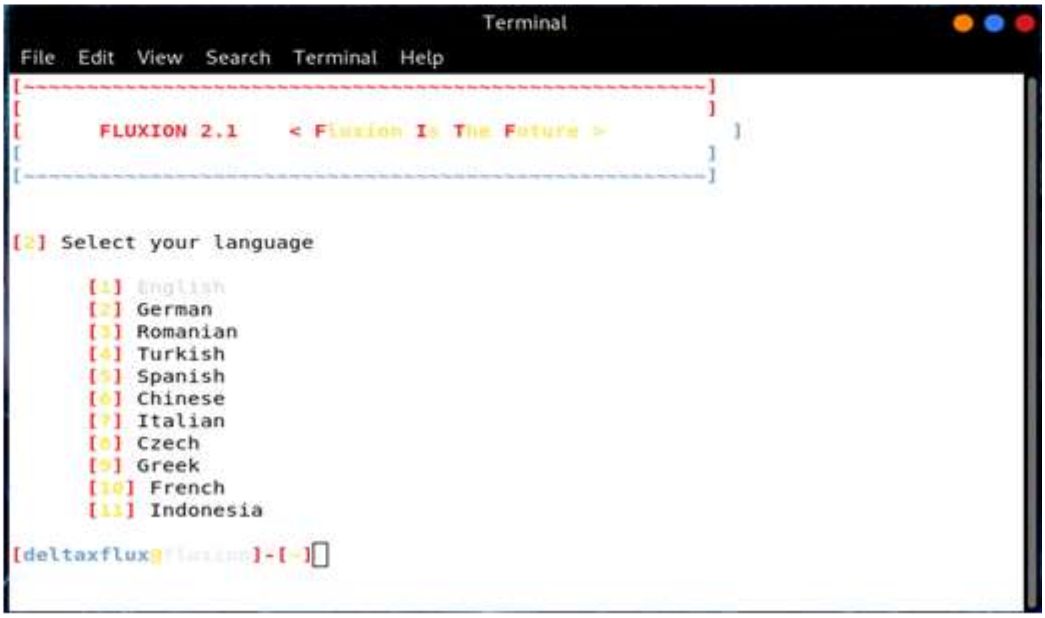
4.1 Fluxion Configurattion.

After the floating stages have been carried out in the Fluxion v2.1 program and a series of trials in the developed section it can be seen that Fluxion already has a choice of Indonesian menus and web interfaces from several router brands circulating in Indonesia and became Fluxion v2.1, as seen on Figure 3, Figure 4 and Figure 5.



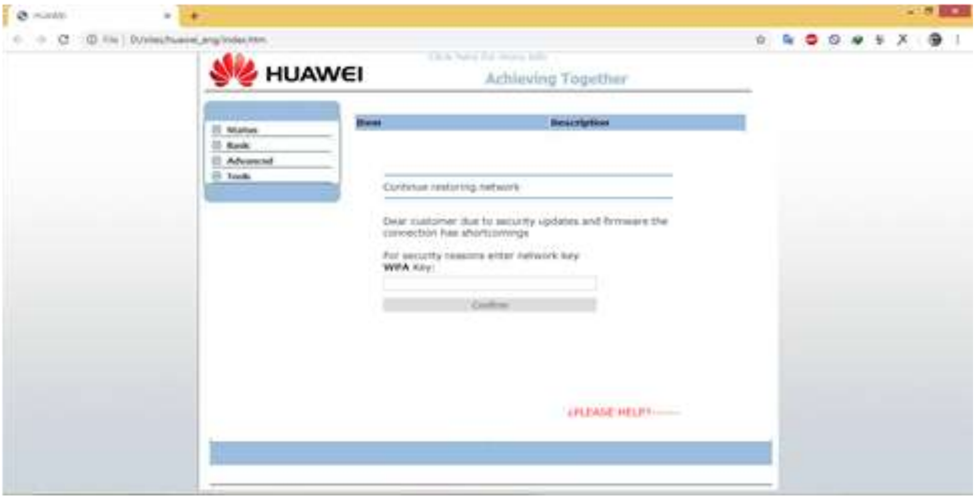
```
FLUXION 2.1    (rev.  9)  by NANDA
Page:https://github.com/FluxionNetwork/fluxion
Latest rev. [?]
```

Figure 3. Fluxion v2.1



```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                          ]
[      FLUXION 2.1    < Fluxion Is The Future >              ]
[                                                          ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]


[2] Select your language

      [1] English
      [2] German
      [3] Romanian
      [4] Turkish
      [5] Spanish
      [6] Chinese
      [7] Italian
      [8] Czech
      [9] Greek
      [10] French
      [11] Indonesia

[deltaxflux@fluxion]-[~]
```

Figure 4. Fluxion v2.1 with Indonesia Language



Continue restoring network

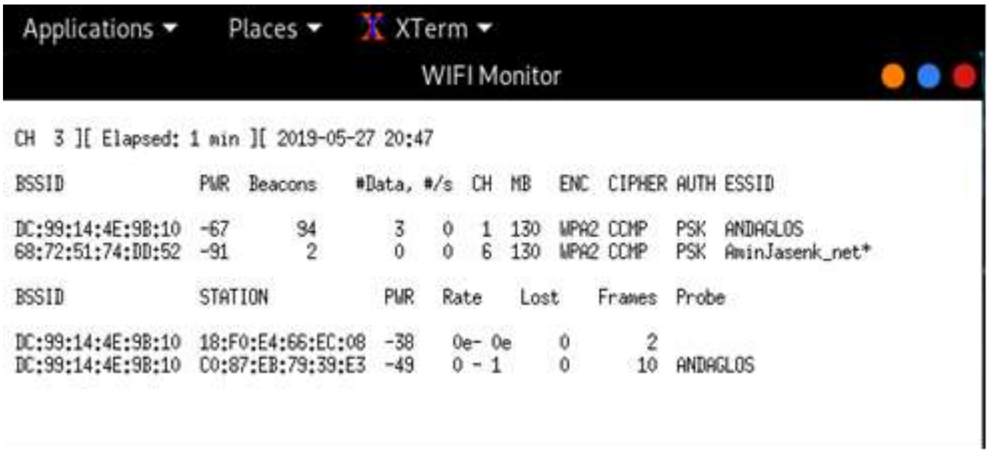
Dear customer due to security updates and firmware the connection has shortcomings

For security reasons enter network key
WPA Key:

¿PLEASE HELP?

Figure 5. Fluxion Web Interfaces.

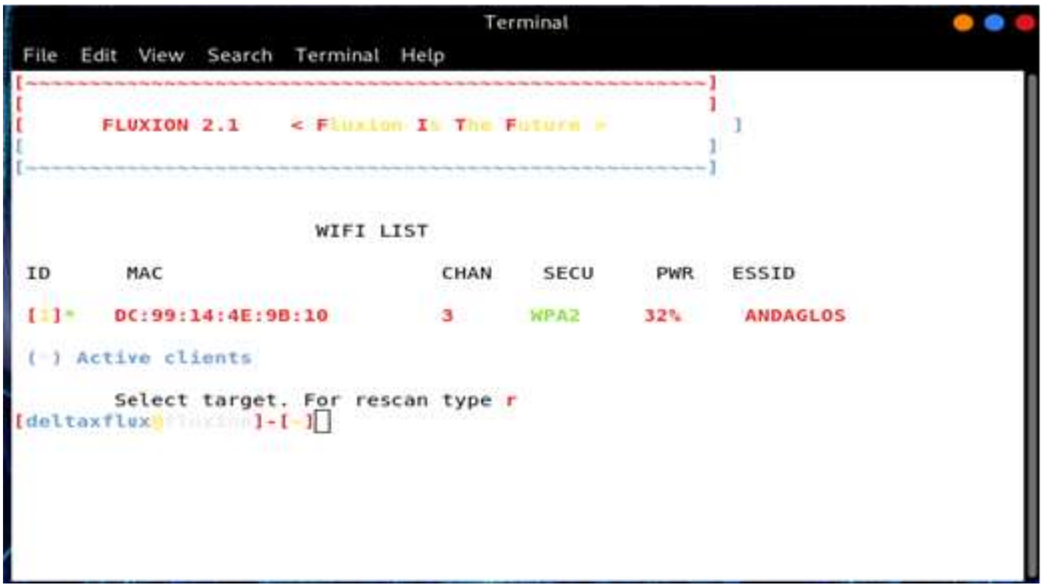
4.2 Penetration Testing.
Network analysis on PT. AGT shows the network power emitted by the router within a radius of 20 meters is at -67/100 dB while the power from the network that can be received by the device or PC client within a 20 meter radius is 33/100 dB so the possibility of failure is high when penetration testing is done, as shown in Figure 6.



```
CH  3 ][ Elapsed: 1 min ][ 2019-05-27 20:47

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

DC:99:14:4E:9B:10  -67       94        3    0   1  130  WPA2 CCMP   PSK  ANDAGLOS
68:72:51:74:DD:52  -91        2        0    0   6  130  WPA2 CCMP   PSK  AminJasenk_net*

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

DC:99:14:4E:9B:10  18:F0:E4:66:EC:08  -38    0e- 0e     0        2
DC:99:14:4E:9B:10  C0:87:EB:79:39:E3  -49    0 - 1      0       10  ANDAGLOS
```

Figure 6. Fluxion WiFi Monitor.

Network selection is very necessary before penetration testing, because there are some networks that cannot be tested if the network does not meet the requirements. The main requirement for Fluxion to test is that there must be a client connected to the network as shown in Figure 7.

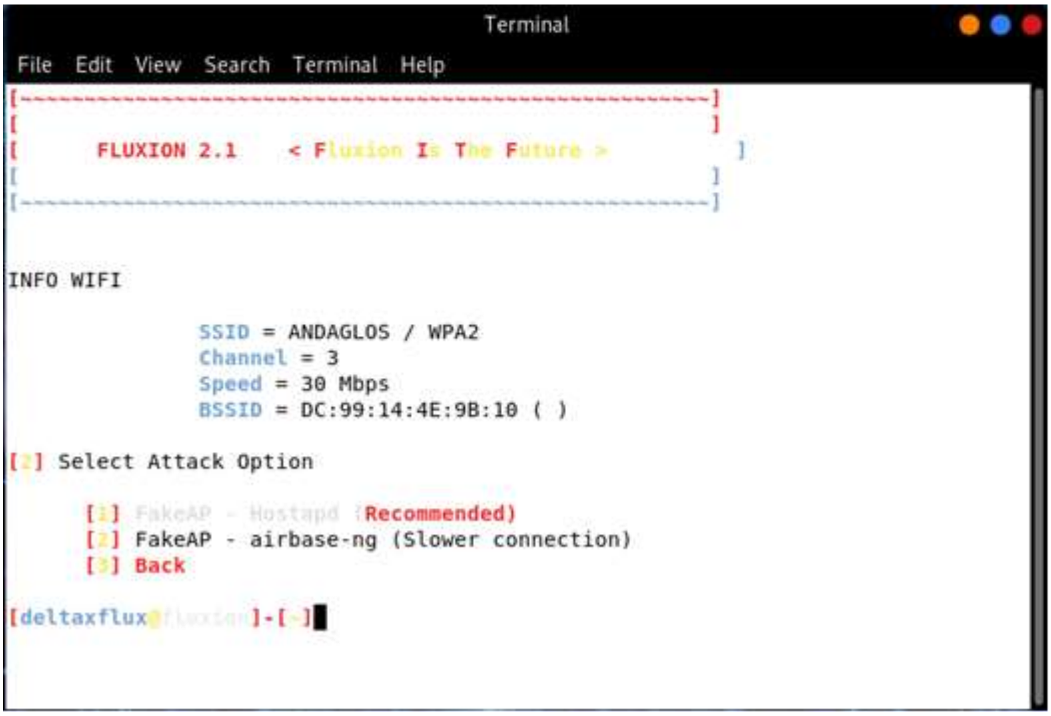


```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                                  ]
[       FLUXION 2.1     < Fluxion Is The Future >                   ]
[                                                                  ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]


                          WIFI LIST

 ID      MAC                        CHAN     SECU      PWR   ESSID

 [1]*   DC:99:14:4E:9B:10          3        WPA2      32%    ANDAGLOS

 (*) Active clients

         Select target. For rescan type r
[deltaxflux@fluxion]-[~]
```

Figure 7. Fluxion Wifi List.

In Figure 4.5 there are 2 different networks and have different colors that can indicate which network has a client and a network that does not have a client. The yellow color on the MAC and the absence of an asterisk next to the number as shown in Figure 7. shows no client connected to the router. The red color on the MAC and the presence of an asterisk next to the number shown in Figure 4.5 shows that there is a client connected to the router.

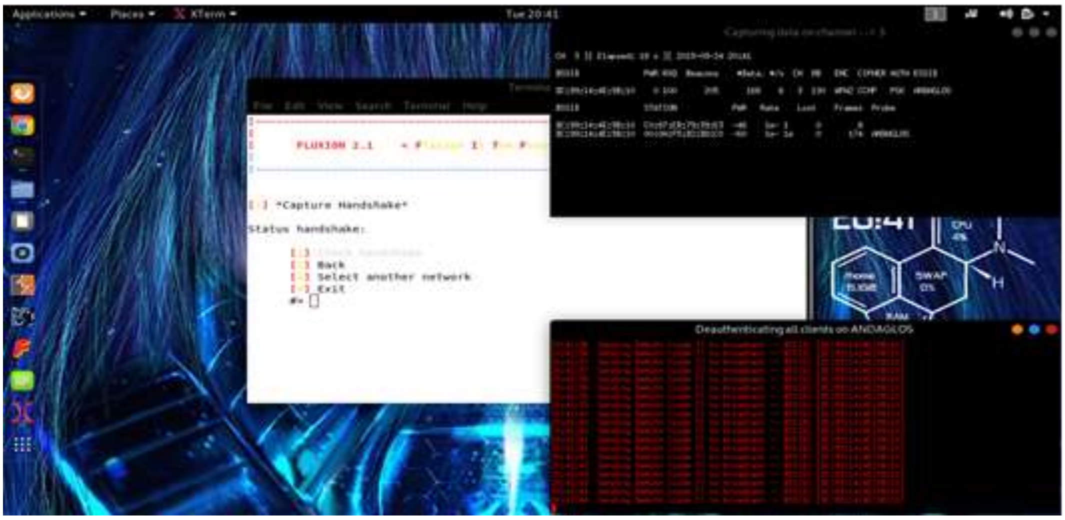
After that making fake access points like in picture 8. is done with two choices, namely: HostAPD and Airbase-ng. HostAPD is a tool that works to make a client an access point, this option is good to use on networks with good signal strength. Airbase-ng is a tool similar to HostAPD, only that Airbase-ng has a high probability of failure when it runs and can only work if the network signal strength is weak.



```
[-----------------------------------------------------------]
[                                                           ]
[      FLUXION 2.1     < Fluxion Is The Future >              ]
[                                                           ]
[-----------------------------------------------------------]


INFO WIFI

               SSID = ANDAGLOS / WPA2
               Channel = 3
               Speed = 30 Mbps
               BSSID = DC:99:14:4E:9B:10 ( )

[2] Select Attack Option

      [1] FakeAP - Hostapd (Recommended)
      [2] FakeAP - airbase-ng (Slower connection)
      [3] Back

[deltaxflux@fluxion]-[~]
```

Figure 8. Fluxion Attack Option.

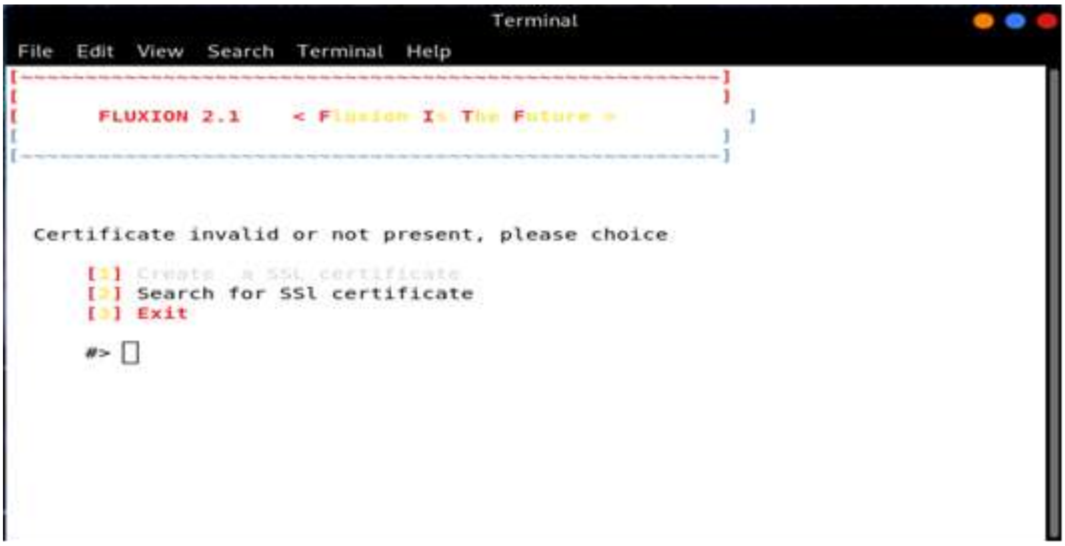
Capture handshake is a process that occurs when a computer will communicate with a foreign device to establish rules for being able to communicate with each other. When the computer communicates with other devices such as a printer, modem, or network server as shown in Figure 9.



```
[-----------------------------------
[
[      FLUXION 2.1     < Fluxion Is The Fu
[
[-----------------------------------

[ ] *Capture Handshake*

Status handshake:

      [1] Check handshake
      [2] Back
      [3] Select another network
      [4] Exit
      #> 
```

Applications
Places
XTerm
Tue 20:41
Capturing data on channel --> 3
Terminal
File Edit View Search Terminal Help
Deauthenticating all clients on ANDAGLOS
CPU
SWAP
RAM

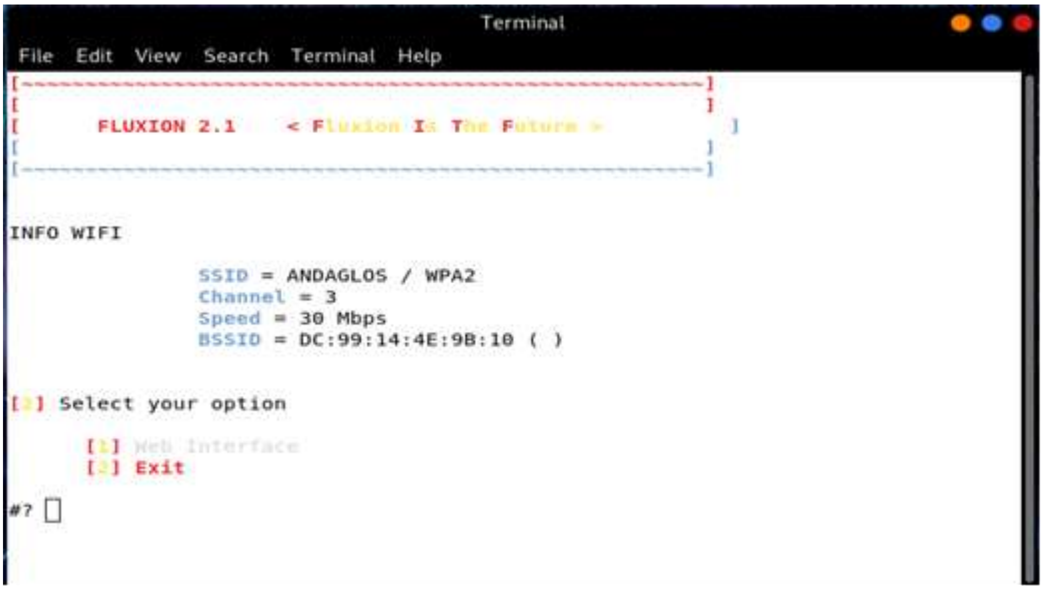
Figure 9. Device Handshake.



```
[------------------------------------------------------------]
[                                                            ]
[       FLUXION 2.1     < Fluxion Is The Future >              ]
[                                                            ]
[------------------------------------------------------------]


  Certificate invalid or not present, please choice

        [1] Create  a SSL certificate
        [2] Search for SSl certificate
        [3] Exit

        #> □
```

Figure 9. Fluxion Create SSL Certification.

Making a web interface that will later be used to trap the client to enter the password on the web page as shown in Figure 10.



```
[------------------------------------------------------------]
[                                                            ]
[       FLUXION 2.1     < Fluxion Is The Future >              ]
[                                                            ]
[------------------------------------------------------------]


INFO WIFI

               SSID = ANDAGLOS / WPA2
               Channel = 3
               Speed = 30 Mbps
               BSSID = DC:99:14:4E:9B:10 ( )

[2] Select your option

      [1] Web Interface
      [2] Exit

#? □
```

Figure 10. Fluxion Creating Web Interface For Fake AP.

The last stage of the Fluxion program is the stage of running the web interface and the monitor will display four terminal windows (figure 11), namely:
1. DHCP which functions to provide ip to the client in order to connect to the fake web interface that we have made.
2. Fake DNS functions as a database to store the ip client so that it can connect to the fake web interface.

3. Deauth All (MDK3) functions to disconnect the client from the router by sending as many packets as possible so that the client is disconnected from the router.
4. WiFi information functions to see whether an active client is accessing the fake web interface.

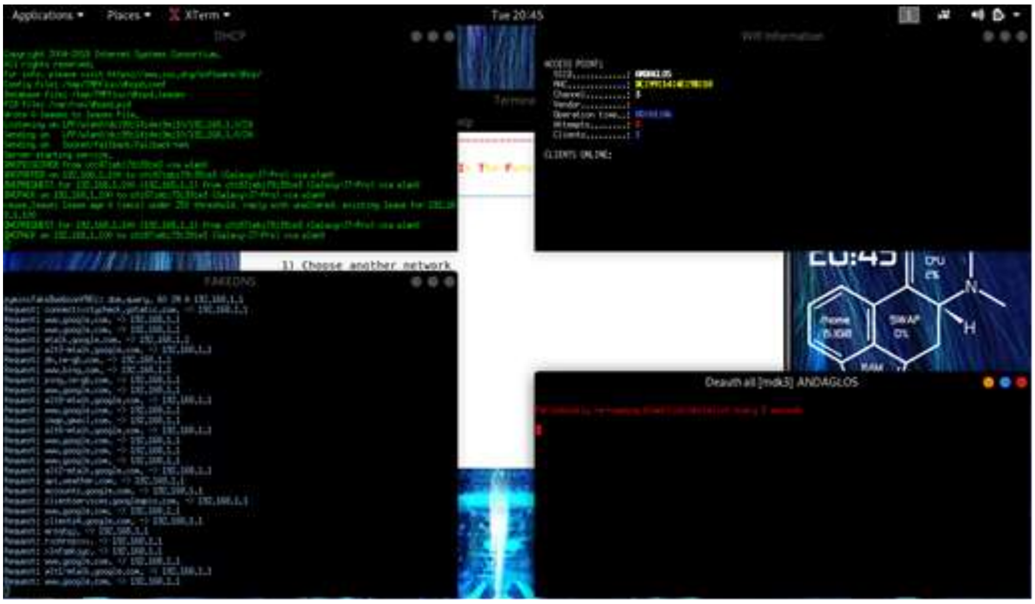
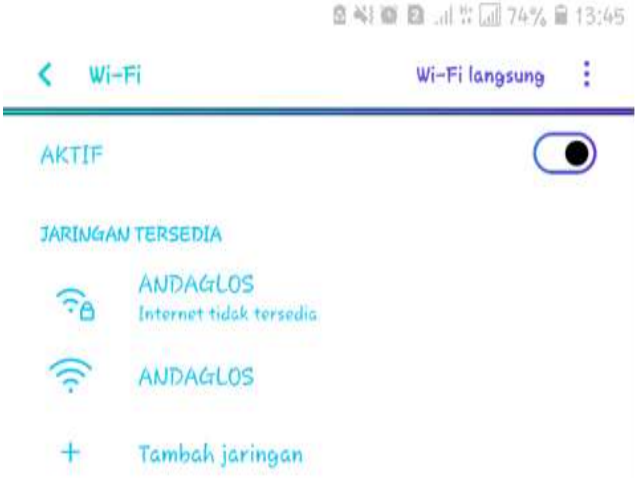


Figure 11. Running Fluxion With Fake AP, Fake Web Login Interfaces.

The client device will display two network options namely the original network and the fake network as shown in Figure 12, where the client cannot connect to the original network and is directed to the fake network. Then the user enters their login information on the fake login web page as shown in Figure 13. Until finally the user login information was successfully obtained by Fluxion as shown in Figure 14.


74% 13:45

Wi-Fi   Wi-Fi langsung

AKTIF

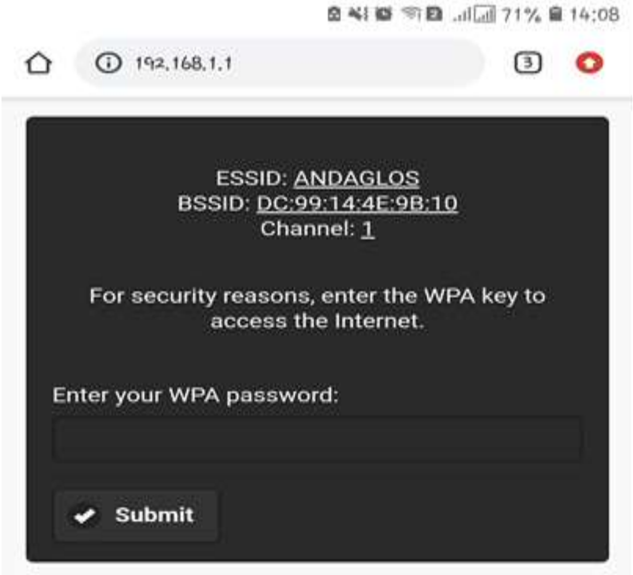
JARINGAN TERSEDIA

ANDAGLOS
Internet tidak tersedia

ANDAGLOS

Tambah jaringan

Figure 12. Fake AP In Client Device.

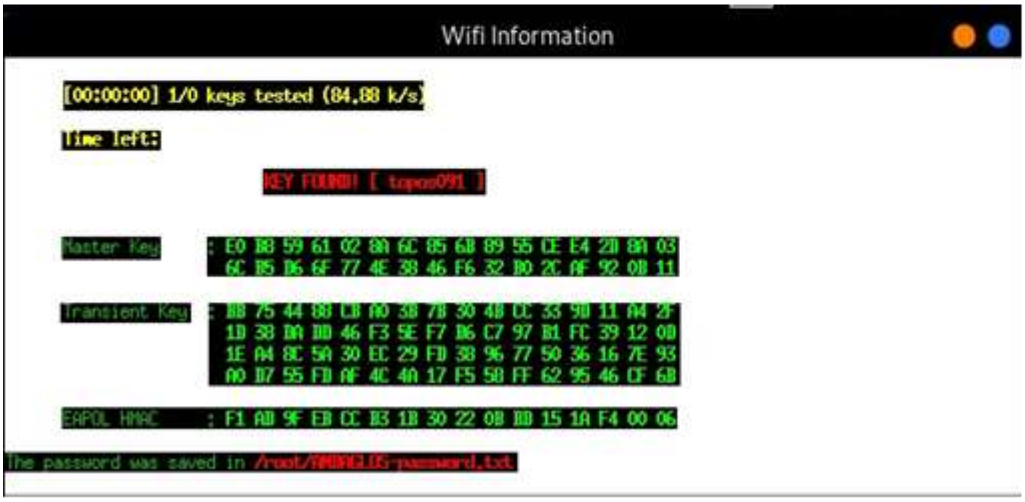


ESSID: ANDAGLOS
BSSID: DC:99:14:4E:9B:10
Channel: 1

For security reasons, enter the WPA key to access the Internet.

Enter your WPA password:

Figure 13. Login Interface In Fake AP.



```
[00:00:00] 1/0 keys tested (84.88 k/s)

Time left:

                    KEY FOUND! [ topos091 ]

Master Key      : E0 B8 59 61 02 8A 6C 85 6B 89 55 CE E4 2D 8A 03
                  6C B5 D6 6F 77 4E 38 46 F6 32 BD 2C AF 92 0B 11

Transient Key   : BB 75 44 8B CB A0 38 7B 30 4B CC 33 9D 11 A4 2F
                  1D 38 DA DD 46 F3 5E F7 B6 C7 97 B1 FC 39 12 0B
                  1E A4 8C 5A 30 EC 29 FD 38 96 77 50 36 16 7E 93
                  A0 D7 55 FD AF 4C 4A 17 F5 5B FF 62 95 46 CF 6B

EAPOL HMAC      : F1 AD 9F EB CC B3 1B 30 22 0B BD 15 1A F4 00 06

The password was saved in /root/ANDAGLOS-password.txt
```

Figure 14. User Login Information Acquired.

5. CONCLUSION

5.1 Fluxion.

Fluxion proved to be very efficient to be used as a penetration testing tool, therefore at this time fluxion is the belle for developers to do penetration testing, so we can conclude:

1. The way the fluxion program works to get passwords is by penetration testing (evil twin) method.
2. The fluxion program is proven to be used to carry out penetration testing on strong and weak networks.
3. Fluxion proved capable of being used as a penetration testing tool and was proven to be able to get a WPA2 security password on a WiFi network at PT.AGT.

5.2 PT AGT Networks.

PT.AGT's network security system does not solve the problem and has gaps in the security of its devices, and the lack of employee knowledge about network security makes the system very likely to be entered by users who take advantage of these weaknesses, therefore conclusions can be drawn:

1. PT.AGT employees do not know when their system has been attacked using Fluxion.
2. PT.AGT employees do not know if an illegal client has entered their router network.
3. PT.AGT only uses standard network setups and does not add any devices such as Mikrotik or create a Gateway for network security.

5.3 Recommendation.

Suggestions for PT. AGT after penetration testing on the system are:

1. Open a network port according to the number of employees employed.
2. Restart the router if it finds that the network has disconnected itself from the router, or when two identical network names are visible on their network.
3. Add the MAC address of the device used by the attacker to the blacklist, so that the device will not be able to connect to the PT.AGT router in the future.
4. Create a gateway password to enter the PT.AGT network system.

REFERENCES

[1] KEAMANAN JARINGAN WLAN TERHADAP SERANGAN WIRELESS HACKING PADA DINAS KOMUNIKASI & INFORMATIKA DIY Vol 1, No 1 (2017): PROSIDING SENSEI 017http://jurnal.unmuhjember.ac.id/index.php/SENSEI17/article/download/844/679

[2] ANALISIS SISTEM KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) PADA PROSES TETHERING Jom FTEKNIK Volume 5 Edisi 2 Juli s/d Desember 2018 https://jom.unri.ac.id/index.php/JOMFTEKNIK/article/download/21865/21159

[3] Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT.PLN (Persero) Wilayah P2B Area Sorong Volume 19 No. 3, Desember 2014 https://ejournal.gunadarma.ac.id/index.php/tekno/article/view/1110

[4] ANALISIS MASALAH KEAMANAN JARINGAN WIRELESS KOMPUTER MENGGUNAKAN CAIN Vol.6 No.1 (2014 http://csrid.potensi-utama.ac.id/index.php/CSRID/article/view/19

[5] SISTEM KEAMANAN JARINGAN NIRKABEL Majalah Ilmiah INFORMATIKA Vol. 3 No. 2, Mei 2012 http://www.unaki.ac.id/ejournal/indesx-php/majalah-ilmiah-informatika/article/download/68/105

[6] PENGEMBANGAN SISTEM PENGAMAN JARINGAN KOMPUTER BERDASARKAN ANALISIS FORENSIK JARINGAN (JITEKI) Vol. 3, No. 1, Juni 2017 http://journal.uad.ac.id/index.php/JITEKI/article/download/5665/3539

[7] ANALISIS KEAMANAN JARINGAN NIRKABEL PUBLIK DENGAN RADIUS (STUDI KASUS UNIVERISTAS SATYA NEGARA INDONESIA – FAKULTAS TEKNIK Vol.13 No 1 Maret 2017 https://lppm.usni.ac.id/jurnal/Jurnal%20Limit-Faizal.pdf

[8] Sistem proteksi Jaringan WLAN Terhadap Serangan Wireless Hacking JRECJournal of Electrical and Electronics Vol. 7 No. 1 http://jurnal.unismabekasi.ac.id/index.php/jrec/article/download/1762/1489/

[9] ANALISIS KELEMAHAN CELAH LAPISAN KEAMANAN PADA JARINGANNIRKABEL Jurnal Ilmiah Media Processor Vol.9 No.1, Februari 2014 http://ejournal.stikom-db.ac.id/index.php/processor/article/download/52/52/

[10] Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas Gadjah Mada) JNTETI, Vol. 1, No. 1, Mei 2012 http://ejnteti.jteti.ugm.ac.id/index.php/JNTETI/article/download/3/2

[11] FLUXION WIFI ANALYZER ORIGINAL PACKAGE https://github.com/FluxionNetwork/fluxion.git