Wireless Implementation on Fake Wifi using Network Forensic Development Life Cycle Method

Richa Retno Rahmadhani Sembiring
Department of Informatics Universitas Ahmad
Dahlan Yogyakarta of Indonesia

Imam Riadi
Department of Information SystemUniversitas
Ahmad Dahlan Yogyakarta of Indonesia

ABSTRACT

Internet technology is growing rapidly, making use of more and more internet networks. From the rapid use of the internet, many attacks or criminal acts committed to attack Internet network aims to steal personal information data. An example of one internet network attack, namely fake wifi where the attack has away the work of duplicating a wifi network with the same SSID name aims gets information from the original wifi by using fluxion tools based on Kali Linux OS. Therefore, to ensnare the perpetrators of crimes against Internet attacks carried out the process of finding evidence and analyzing it. This research uses the Network Forensics Development Life method Cycle (NFDLC) with several stages, namely Initiations, Acquisition, Implementation, Operations, and Disposition. This research uses tools Wireshark for the monitoring process and forfurther analysis using Network Miner tools that can analyze traffic or files suspiciously. The research results obtained from the NFDLC method are starting with analyzing the equipment used, attack flowcharts and investigation, attack simulation, and monitoring analysis results. Analysis results the last one shows that there are some suspicious files such as HTML files and CSS. The last analysis is how the difference between real and fake wifi is for example in termsof security and also the victim is directed to the websitepage enter wifi if victim access fake wifi

Keywords

Fake Wifi, NFDLC,Wireshark, Network Miner, Wifi

1. INTRODUCTION

Wireless technology offers a widerange of convenience, high flexibility, and freedom. Wireless technology has many advantages over existing cable technology, for example, the ease of access to data communication and internet access in any area as long as it is still within wireless range [1]. Devicesconnected to the internet network will get more than triple the number, such as home assets, autonomous cars, medical devices, and others [2]. With the rapid development, the number of internet users will increase. According to a survey report compiled by the Indonesian Internet Service Providers Association (APJII) in Indonesia internet use in 2020 reached

196.7 million people out of a total of 273.5 million people in the entire population of Indonesia where this number increased by 23.5 million people or 8.9% compared to 2018.Wireless networks pose a more critical security risk thancable networks because the air medium in a wireless network cannot be physically controlled [3]. This makes the attackers or hackers become interested indoing activities on wireless networks. Attacks carried out by utilizing fake AP (Acces Point) or called fake wifi process is made the same as access point attack location so that the perpetrator more easily launches illegal attacks[4]. Fake wifi or Fake Access Point is a serious security threat resulting from unauthorized access connected to a company's network [5]. The wireless network attack was carried out by mimicking the name of the original wifi network at the scene, but in fact, hackers have been created to intercept wireless communications among internet surfers [6]. Network and sniff information using fake wifi. Perpetrators of crimes on fake wifi can be acted on by the law for illegal behavior committed, but to punish the perpetrator requires evidence.

2. STUDY LITERATURE

2.1 Network Forensics

Network Forensics is analyzing an eventon a network with the activity of analyzing, capturing, and recording to find security or problems and find the source of other incident attacks [7]. The power of forensics is to recover facts from events that occurred and rediscover facts that may have been hidden [8]. Unlike forensics in general, computer forensics is the activity of collecting and analyzing data from various computer resources [9]. Network traffic data is captured using packet sniffers, alerts,and logs collected from existing network security tools. This data is analyzed for the characterization of the attack and investigated to trace back the offender. Prosecution through forensicallycomplete evidence and providing an understandingof the root causes of security breaches to enable prompt, intelligent, and effective responses to prevent catastrophic events and ongoing risks. This allows for improvement after a breach occurs through theability to replay network attacks [10]. In many cases, certain crimes do not violate network security policies but can be prosecuted legally. Such crimes can only be dealt with by networkforensics [11].

2.2 Wireless Network

which is based on the specificationsof The Institute of Electrical and Electronics Engineer (IEEE) 802 and the general public calls it wi-fi is a network that can connect a device either the computer or laptop or other media to connect with other devices without having to connect to a network cable [12]. Connected network systems use electromagnetic waves as their medium [13]. Wireless Internet is an Internet service thatcan be accessed withouta physical wired connection to a computer using the Internet by using a wireless card (wireless card) or Personal Digital Assistant (PDA) to connect to the internet that utilizes the nearest hotspot access point [14].

2.3 Fake Wifi

Fake Wifi or Fake Access point is the act of accessing unauthorized lines connected to a company's network that pose aserioussecurity threat [15]. Fake Wifi attack is to createfake wifi that simulates the real wifi [16]. The difference between real and fake wifi is the signal strength where the fake wifi increases the amount of power transmitted to ensure long- distance range [17]. The original Wifi can be used at a level ofsecurity, such as WEP, WPA I, or WPA II to protect the Wifi network [18]. Rogue Access Points are set up on a network without permission from administrators and utilize conventional automatic access point selection techniques to create wireless networks to have victims connected to Rogue Access Point [19].

3. METHODS

3.1. Attack Simulation

Making fake wifi is done using Kali Linux operating system that utilizes fluxion tools where these tools can create aninterface for password page that will appear when the victim accesses the fake wifi network. That's when the password information original data wifi acceptable to the attacker.

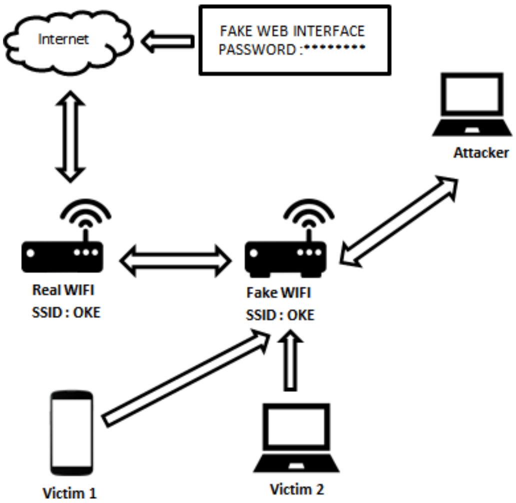


Figure 1. Attact Simulation

Figure 1 describes the fake wifi attack scheme where there isa wifi network with the SSID "OK" which has an internet network and security in the form of a password, then there is an assailant who takes action duplicate “OK” wifi network without security so potential victims are provoked to access the fake wifi network. Fake wifi is created using fluxion tools which in it can create an interface page on when the victim accesses the fake wifi, it is immediately directed to a page so that the victim enters the original password. So that attackers can find out information in the form of passwords from the original wifi he duplicated. Victims of this attack can use various devices, for example in Figure 1 namely cell phones and laptops.

The method used in this study to perform the Fake Wifi attack analysis process using the Network Forensics Development Life Cycle (NFDLC) method. This method can be described in Figure 2.

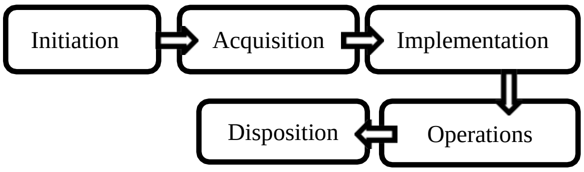


Figure 2. Network Forensics Development Life Cycle

Figure 2 is a stage of the Network Forensic Development Life Cycle (NFDLC) method. The explanation of each stage can be explained as follows:

1) Initiation is to determine aspects of the network in digital forensic protection to beanalyzed.

2) Acquisition / Development is the process of building or building a system that contains evidence rules in the system, as well as verifying and calibrating the system.

3) Implementation is the basic testing of a platform by verifying network mechanisms.

4) Operations/Maintenance is a process of examination, verification, and measurement taken against the use of the network as digital evidence.

5) Disposition is performing procedures to secure evidence on forensic tissue.

4. RESULT AND DISCUSSION

4.1. Initiation

The initiation stage is the initial stage of the search, the collection of data needed in thisstudy up to the documenting of evidence. Objects used for research as evidence of forensicnetwork i.e. Wifi or Access Point. The results of wi network monitoring will be analyzed and then collected data log results from the ARP and HTTP protocols.There is some equipment which is divided into two parts, namely software (software) and hardware (hardware). Requirement specifications can be described as follows:

1) Software

The software that will be used in the research components as contained in Table 1 Device Requirements Software.

Table 1. Software Requirements

No	Software	Description
1	OS Windows 10 Profesional	Victim PC OS
2	Android 6.0.1	Victim PC OS
3	Kali Linux 2021.4a	Attacker PC OS
4	Fluxion 6.9	Fake Wifi Attack Tools
5	Wireshark	Monitoring Tools
6	Network Miner	Tools Analysis of monitoring results

2) Hardware

Hardware requirements used for forensic needs in this study are described as contained in Table 2.

Table 2. Hardware Requirements

No	Hardware	Description
1	Lenovo Ideapad 110 Laptop	Attacker
2	Samsung Galaxy J2	Victim 1
3	HP Laptop	Victim 2
4	USB V-Gen 32GB	Tools for Kali Linux installation
5	Modem Indihome Huawei HG8245A	Acces Point

4.2. Acquisition

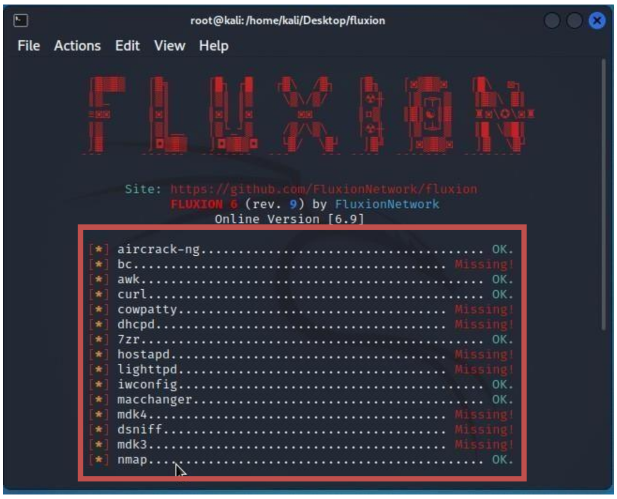
At this stage, the installation process and configuration of the system will be used in the research. The installation of the system can be explained as follows:

4.2.1. Kali Linux 2021.4a

Kali Linux 2021.4a installation stage can use a live CD, via USB and can also virtual machine. Kali Linux OS can be downloaded through the official website of www.kali.org/get- kali/. Then select Bare Metal to download Kali Linux with ISO Format. Next created Bootable USB to perform the Process of Installing Kali Linux on an Attacker PC

4.2.2. Fluxion 6.9

Fluxion is a tool to duplicate wifi to getinformation from the original wifi. Theinstallation process is carried out inside the Kali Linux Operating System on the Attacker PC. The initial stage of the process is to firstopen the terminal on the toolbar then enter theroot with the command "sudo su" and then clone the file on the website https://github.com/ Fluxion Network/ fluxion with the command "git clone". progress to run fluxion where previouslyit had to enter the fluxion folder with the command "cd fluxion" than to run it using the command "./fluxion.sh" on the terminal that can be seen in Figure 3.



```
Site: https://github.com/FluxionNetwork/fluxion
FLUXION 6 (rev. 9) by FluxionNetwork
Online Version [6.9]

[*] aircrack-ng.................................. OK.
[*] bc..................................... Missing!
[*] awk.......................................... OK.
[*] curl......................................... OK.
[*] cowpatty............................... Missing!
[*] dhcpd.................................. Missing!
[*] 7zr.......................................... OK.
[*] hostapd................................ Missing!
[*] lighttpd............................... Missing!
[*] iwconfig..................................... OK.
[*] macchanger................................... OK.
[*] mdk4................................... Missing!
[*] dsniff................................. Missing!
[*] mdk3................................... Missing!
[*] nmap......................................... OK.
```

Figure 3. Fluxion Home Page on Kali Linux

4.3. Implementation

Implementation is the basic testing process of making an investigative flowchart and an assault flowchart that will be carried out in the research. Implementation and maintenance is the final stage in making Network Forensics DevelopmentLife Cycle (NFDLC). At this stage, the system has been created, tested, and confirmed to work optimally. After the manufacturing phase is complete, implementation and maintenance are carried out by the user.

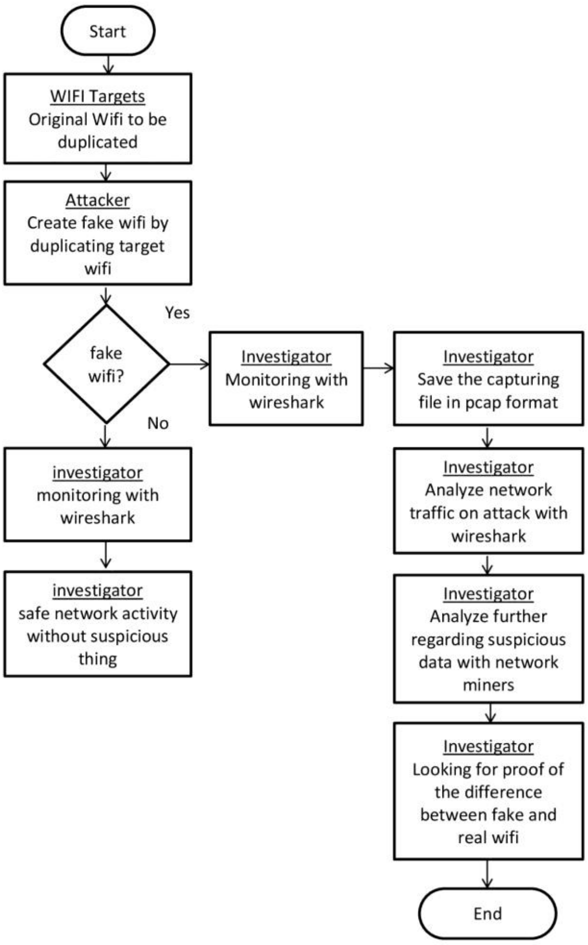

Start
WIFI Targets
Original Wifi to be duplicated
Attacker
Create fake wifi by duplicating target wifi
fake wifi?
Yes
No
Investigator
Monitoring with wireshark
Investigator
Save the capturing file in pcap format
investigator
monitoring with wireshark
Investigator
Analyze network traffic on attack with wireshark
investigator
safe network activity without suspicious thing
Investigator
Analyze further regarding suspicious data with network miners
Investigator
Looking for proof of the difference between fake and real wifi
End

Figure 4. Flowchart of Investigation Scenario

Figure 3 is an investigative flowchart for this fake wifi attack using several tools namely Wireshark and Network Miner.

1) In the initial scenario the attacker targets the original wifi which will be done the process of duplicating wifi.

2) Then the attacker creates fake wifi with the same SSID name as the original wifi.

3) Then if the investigator accesses the original wifi thenwhen monitoring the network with the Wireshark application does not find anything suspicious in the network traffic.

4) But if the investigator accesses fake wifi then the monitoring process is carried out for a few minutes then saves the results inthe format *.pcap.

5) The monitoring results are then analyzed using Wireshark tools by analyzing suspicious activity from network trafficon HTTP ports, ARP ports, and mediapresentation ports.

6) After that further analysis in finding somesuspicious files such as HTML, CSS, jpg, and png files can be done using network miner tools.

7) Next the last stage of analysis is to determine some differences between fake wifi and real wifi with examples in terms of security and the process of how the flow in accessing wifi.

4.3.1. Flowchart Investigation

The investigation flowchart is the process flow of how the investigation into the fake wifi case analysis is carried out. The investigator also plays the victim's role and acts like a victim so the attacker doesn't feel suspicious. From the results of the investigation obtained, there are several reports that have been arrested by the investigators, namely in the form of network flows, data files obtained and some evidence of differences in the fake or original wifi networks. So that the evidence obtained can be used as material to report the attacker.

4.3.2. Flowchart Attack

The attack flowchart is the flow process of how theattacker commits his crime against several victims. The goal is to get some information for the benefit of the attacker.

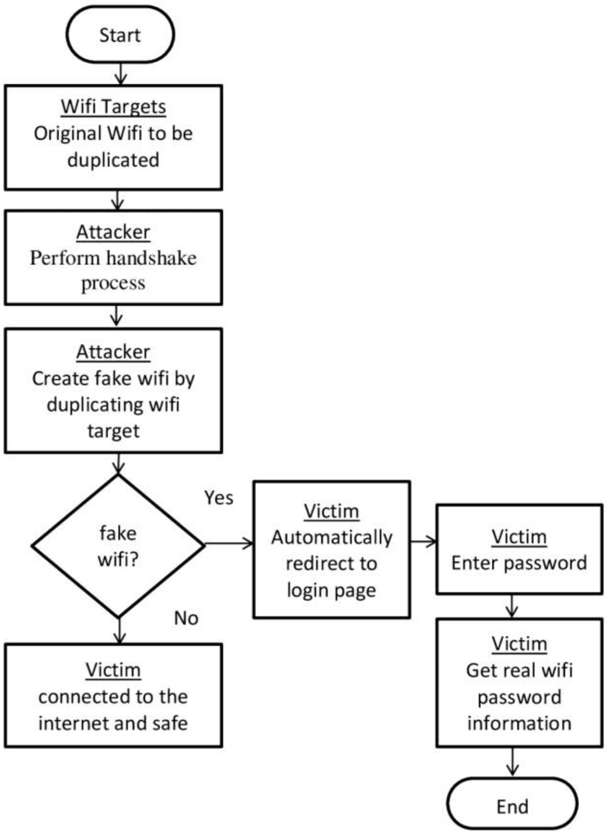

Start
Wifi Targets
Original Wifi to be duplicated
Attacker
Perform handshake process
Attacker
Create fake wifi by duplicating wifi target
fake wifi?
Yes
No
Victim
Automatically redirect to login page
Victim
Enter password
Victim
Get real wifi password information
End
Victim
connected to the internet and safe

Figure 5. Flowchart of Attack Scenario

In Figure 5 the flowchart of the attackwas carried out on the perpetrator by targeting the victim who tried to access a wifi network.

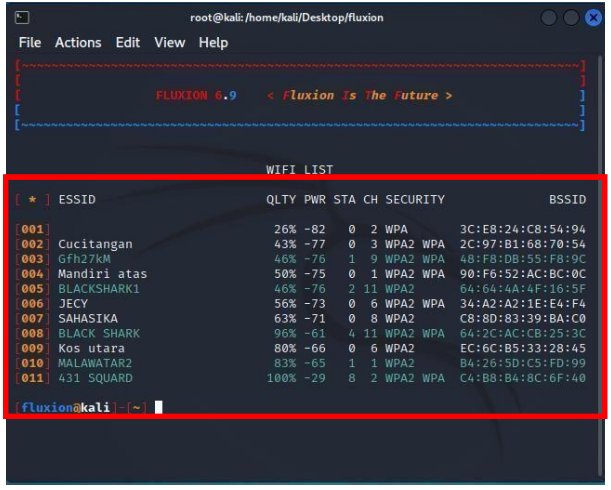
1) In the initial scenario the attacker targets the original wifi which will be done the process of duplicating wifi.
2) Then the attacker performs the handshake process whichis an introductory system that occurs between one device and another, thus allowing the device to be connected and can exchange data.
3) then the attacker creates fake wifi with the same SSID name as the original wifi.
4) Then if the victim accesses the original wifi then he can connect to the internet and walk safely.
5) If the victim accesses the wrong wifi then it is automatically sidetracked to the fake web page to enter the password.
6) Furthermore, the attacker gets information in the form of a password from the original wifi and also the victim's IP address.

4.4. Operations

Operations are the main process carried out in this research such as conducting attacks and monitoring attacks.

4.4.1. Handshake

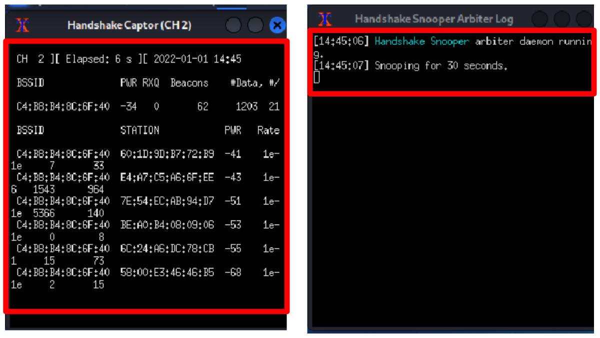
The handshake process carried out by theattacker to carry out the recognition process that occurs between one device and another device, allowing the device to be connected and can exchange data to obtain information from security on the wifi network. [20]. A handshakeis a wireless digital handshake that occurs between two or more devices. A handshake goes through 3 stages of the process carried out by these machines when "acquainted" to connect. So what we need to hack wifi passwords with WPA/WPA2 security.


root@kali: /home/kali/Desktop/fluxion
File Actions Edit View Help

```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                                         ]
[                FLUXION 6.9     < Fluxion Is The Future >                ]
[                                                                         ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]

                             WIFI LIST

[ * ] ESSID                       QLTY PWR STA CH SECURITY           BSSID

[001]                              26% -82   0  2 WPA      3C:E8:24:C8:54:94
[002] Cucitangan                   43% -77   0  3 WPA2 WPA 2C:97:B1:68:70:54
[003] Gfh27kM                      46% -76   1  9 WPA2 WPA 48:F8:DB:55:F8:9C
[004] Mandiri atas                 50% -75   0  1 WPA2 WPA 90:F6:52:AC:BC:0C
[005] BLACKSHARK1                  46% -76   2 11 WPA2     64:64:4A:4F:16:5F
[006] JECY                         56% -73   0  6 WPA2 WPA 34:A2:A2:1E:E4:F4
[007] SAHASIKA                     63% -71   0  8 WPA2     C8:8D:83:39:BA:C0
[008] BLACK SHARK                  96% -61   4 11 WPA2 WPA 64:2C:AC:CB:25:3C
[009] Kos utara                    80% -66   0  6 WPA2     EC:6C:B5:33:28:45
[010] MALAWATAR2                   83% -65   1  1 WPA2     B4:26:5D:C5:FD:99
[011] 431 SQUARD                  100% -29   8  2 WPA2 WPA C4:B8:B4:8C:6F:40

[fluxion@kali]-[~]
```

Figure 6. Result of Scanning Wifi

Figure 6 shows a list of results from the previous scan by pointing to information from each wifi. At this stage, the attacker chooses which wifi network to choose for the handshake process and this research is to choose menu number 11.



```
 CH  2 ][ Elapsed: 6 s ][ 2022-01-01 14:45

 BSSID              PWR RXQ  Beacons    #Data, #/

 C4:B8:B4:8C:6F:40  -34   0       62     1203  21

 BSSID              STATION            PWR   Rate

 C4:B8:B4:8C:6F:40  60:1D:9D:B7:72:B9  -41    1e-
1e     7         33
 C4:B8:B4:8C:6F:40  E4:A7:C5:A6:6F:EE  -43    1e-
6   1543        964
 C4:B8:B4:8C:6F:40  7E:54:EC:AB:94:D7  -51    1e-
1e  5366        140
 C4:B8:B4:8C:6F:40  BE:A0:B4:08:09:06  -53    1e-
1e     0          8
 C4:B8:B4:8C:6F:40  6C:24:A6:DC:78:CB  -55    1e-
1     15         73
 C4:B8:B4:8C:6F:40  58:00:E3:46:46:B5  -68    1e-
1e     2         15
```

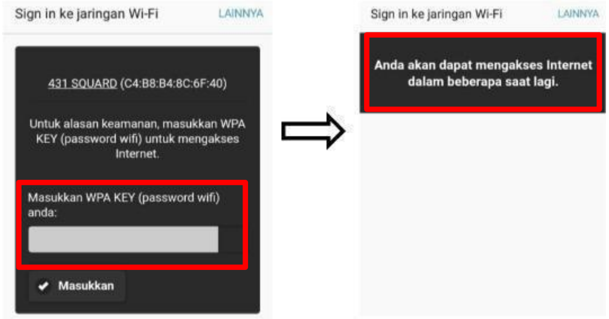
```
[14:45:06] Handshake Snooper arbiter daemon runnin
g.
[14:45:07] Snooping for 30 seconds.
```

Figure 7. Handshaking Progress

The handshake process in Figure 7 is checked every 30 seconds until the handshake process is complete. And after that, the processcan be continued with the creation of fake wifi.

4.4.2. Fake Wifi

Fake Wifi is to create a fake wifi network which is an illegal activity carried out by someone with the purpose of crime to get information as in this study that is thepassword of the original wifi [21]. On the home page of the menu on the fluxion tools. After the handshake process, the next stage is the process of making fake wifi [22]. Fake Wifi can be created by selecting the Captive Portal menu. Thenchoose the deauthentication process method to disconnect the wifi and in this study use theaireplay method. After that select the attack option on Access Point. In this study, rogue- AP hostapd is an access point pen tester/attacker software that is able to convert network interface cards into access points and authentication servers [23]. To attack the targeted wifi to crack the WPA2-PSKpassword of the wifi with the result of encryption in the form of a code. The study selected the hash-cowpatty method by simplifying and speeding up attacks on passwords that then generate code from the encryption process. An SSL certificate (Secure Sockets Layer) is a digital certificate that authenticates a website's identity and encrypts information sent to a server using SSL technology [24].



Sign in ke jaringan Wi-Fi
LAINNYA

431 SQUARD (C4:B8:B4:8C:6F:40)

Untuk alasan keamanan, masukkan WPA KEY (password wifi) untuk mengakses Internet.

Masukkan WPA KEY (password wifi) anda:

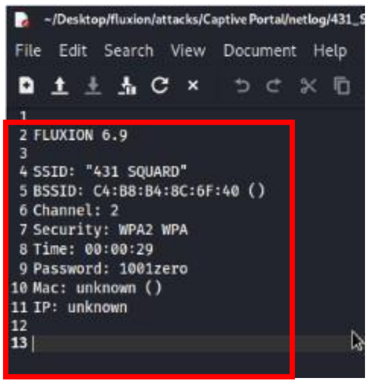
✓ Masukkan

Sign in ke jaringan Wi-Fi
LAINNYA

Anda akan dapat mengakses Internet dalam beberapa saat lagi.

Figure 8. Login Page on The Victim Device

In Figure 8 when the victim accessesa fake wifi network, it will be directed to an entry page where it has a form to enter the password of the wifi. And after success, the next page that is the victim will be ordered to wait a while to access the internet, but this is not the case. After that, the attacker gets the password information from the original wifi inputted.



~/Desktop/fluxion/attacks/Captive Portal/netlog/431_S
File Edit Search View Document Help

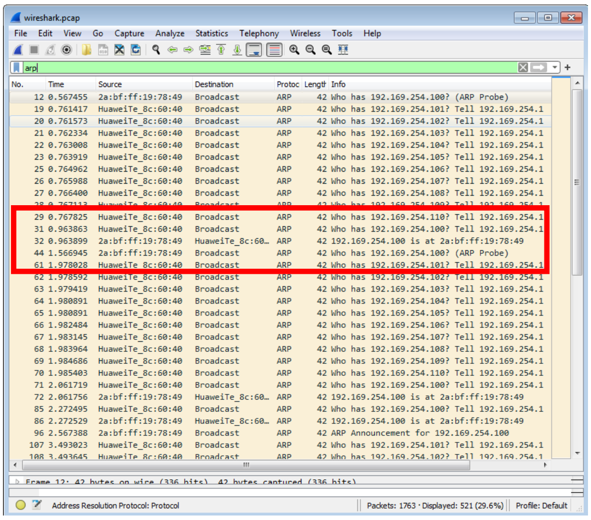
```

FLUXION 6.9

SSID: "431 SQUARD"
BSSID: C4:B8:B4:8C:6F:40 ()
Channel: 2
Security: WPA2 WPA
Time: 00:00:29
Password: 1001zero
Mac: unknown ()
IP: unknown


```

Figure 9. Results of Fake Wifi Attack

After the attack process is complete, the attacker can see information from the original wifi that can be seen in Figure 8in the folder that has been directed from the fluxion tool. Itcan be seen that the information has SSID from wifi, BSSID or Mac Address from SSID, channel information from wifi, the type of security of the original wifi, the time obtained during the process of getting the original wifi information, and password from the original wifi.

4.4.3. *Monitoring*

Proof of monitoring live or directly using the Wireshark application whose results are stored is then analyzed further using the Network Miner application. The analysis process is done by utilizing hierarchical modules and command- command filtering packages from Wireshark tools [25]. The results of the hierarchy table analysis there are 3 objects that can be used as analytical materials, namely THE HTTP Protocol, Protocol ARP, and Media Presentation Protocol. The ARP protocol is used to translate IP addresses into MAC addresses. The HTTP protocol is a website component that regulates the exchange of data that takes place on the internet.



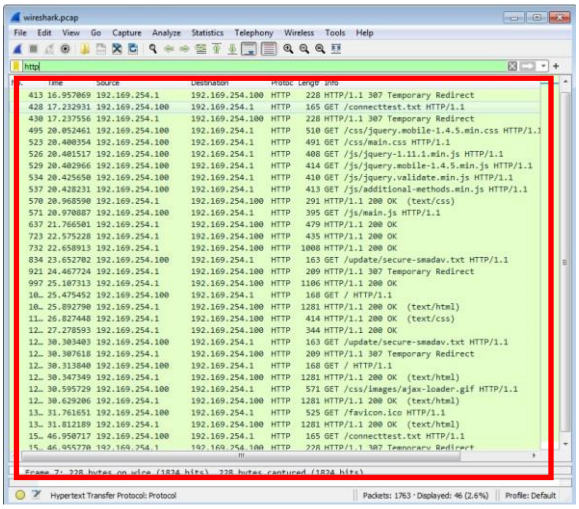
wireshark.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

```
No.   Time      Source             Destination        Protoc Length Info
   12 0.567455  2a:bf:ff:19:78:49  Broadcast          ARP    42 Who has 192.169.254.100? (ARP Probe)
   19 0.761417  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.101? Tell 192.169.254.1
   20 0.761573  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.102? Tell 192.169.254.1
   21 0.762334  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.103? Tell 192.169.254.1
   22 0.763008  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.104? Tell 192.169.254.1
   23 0.763919  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.105? Tell 192.169.254.1
   25 0.764962  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.106? Tell 192.169.254.1
   26 0.765988  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.107? Tell 192.169.254.1
   27 0.766400  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.108? Tell 192.169.254.1
   28 0.767113  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.109? Tell 192.169.254.1
   29 0.767825  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.110? Tell 192.169.254.1
   31 0.963863  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.100? Tell 192.169.254.1
   32 0.963899  2a:bf:ff:19:78:49  HuaweiTe_8c:60…    ARP    42 192.169.254.100 is at 2a:bf:ff:19:78:49
   44 1.566945  2a:bf:ff:19:78:49  Broadcast          ARP    42 Who has 192.169.254.100? (ARP Probe)
   61 1.978028  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.101? Tell 192.169.254.1
   62 1.978592  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.102? Tell 192.169.254.1
   63 1.979419  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.103? Tell 192.169.254.1
   64 1.980891  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.104? Tell 192.169.254.1
   65 1.980891  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.105? Tell 192.169.254.1
   66 1.982484  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.106? Tell 192.169.254.1
   67 1.983145  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.107? Tell 192.169.254.1
   68 1.983964  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.108? Tell 192.169.254.1
   69 1.984686  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.109? Tell 192.169.254.1
   70 1.985403  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.110? Tell 192.169.254.1
   71 2.061719  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.100? Tell 192.169.254.1
   72 2.061756  2a:bf:ff:19:78:49  HuaweiTe_8c:60…    ARP    42 192.169.254.100 is at 2a:bf:ff:19:78:49
   85 2.272495  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.100? Tell 192.169.254.1
   86 2.272529  2a:bf:ff:19:78:49  HuaweiTe_8c:60…    ARP    42 192.169.254.100 is at 2a:bf:ff:19:78:49
   96 2.567388  2a:bf:ff:19:78:49  Broadcast          ARP    42 ARP Announcement for 192.169.254.100
  107 3.493023  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.101? Tell 192.169.254.1
  108 3.493645  HuaweiTe_8c:60:40  Broadcast          ARP    42 Who has 192.169.254.102? Tell 192.169.254.1

▷ Frame 12: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

Address Resolution Protocol: Protocol    Packets: 1763 · Displayed: 521 (29.6%)    Profile: Default
```

Figure 10. Monitoring Results on ARP Protocol

Figure 10 shows the ARP protocol from the monitoring results on a wifi network. Where is the ARP protocol which is used to translate IP addresses into MAC address How does it work with the sending host ARP Request broadcast to get MAC address destination hosts. in the picture shows that the existence of ARP activities broadcast from 2a:bf:ff:19:78:49 with IP Address 192.169.254.100 trying to contact MAC Address Destination HuaweiTe_8c:60:40 with IP 192.169.254.1.



wireshark.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.   Time       Source           Destination      Protoc Length Info
  413 16.957069 192.169.254.1    192.169.254.100  HTTP   228 HTTP/1.1 307 Temporary Redirect
  428 17.232931 192.169.254.100  192.169.254.1    HTTP   165 GET /connecttest.txt HTTP/1.1
  430 17.237556 192.169.254.1    192.169.254.100  HTTP   228 HTTP/1.1 307 Temporary Redirect
  495 20.052461 192.169.254.100  192.169.254.1    HTTP   510 GET /css/jquery.mobile-1.4.5.min.css HTTP/1.1
  523 20.400354 192.169.254.100  192.169.254.1    HTTP   491 GET /css/main.css HTTP/1.1
  526 20.401517 192.169.254.100  192.169.254.1    HTTP   408 GET /js/jquery-1.11.1.min.js HTTP/1.1
  529 20.402966 192.169.254.100  192.169.254.1    HTTP   414 GET /js/jquery.mobile-1.4.5.min.js HTTP/1.1
  534 20.425650 192.169.254.100  192.169.254.1    HTTP   410 GET /js/jquery.validate.min.js HTTP/1.1
  537 20.428231 192.169.254.100  192.169.254.1    HTTP   413 GET /js/additional-methods.min.js HTTP/1.1
  570 20.968590 192.169.254.1    192.169.254.100  HTTP   291 HTTP/1.1 200 OK  (text/css)
  571 20.970887 192.169.254.100  192.169.254.1    HTTP   395 GET /js/main.js HTTP/1.1
  637 21.766501 192.169.254.1    192.169.254.100  HTTP   479 HTTP/1.1 200 OK
  723 22.575228 192.169.254.1    192.169.254.100  HTTP   435 HTTP/1.1 200 OK
  732 22.658913 192.169.254.1    192.169.254.100  HTTP  1008 HTTP/1.1 200 OK
  834 23.652702 192.169.254.100  192.169.254.1    HTTP   163 GET /update/secure-smadav.txt HTTP/1.1
  921 24.467724 192.169.254.1    192.169.254.100  HTTP   209 HTTP/1.1 307 Temporary Redirect
  997 25.107313 192.169.254.1    192.169.254.100  HTTP  1106 HTTP/1.1 200 OK
  10… 25.475452 192.169.254.100  192.169.254.1    HTTP   168 GET / HTTP/1.1
  10… 25.892790 192.169.254.1    192.169.254.100  HTTP  1281 HTTP/1.1 200 OK  (text/html)
  11… 26.827448 192.169.254.1    192.169.254.100  HTTP   414 HTTP/1.1 200 OK  (text/css)
  12… 27.278593 192.169.254.1    192.169.254.100  HTTP   344 HTTP/1.1 200 OK
  12… 30.303403 192.169.254.100  192.169.254.1    HTTP   163 GET /update/secure-smadav.txt HTTP/1.1
  12… 30.307618 192.169.254.1    192.169.254.100  HTTP   209 HTTP/1.1 307 Temporary Redirect
  12… 30.313840 192.169.254.100  192.169.254.1    HTTP   168 GET / HTTP/1.1
  12… 30.347349 192.169.254.1    192.169.254.100  HTTP  1281 HTTP/1.1 200 OK  (text/html)
  12… 30.595729 192.169.254.100  192.169.254.1    HTTP   571 GET /css/images/ajax-loader.gif HTTP/1.1
  12… 30.629206 192.169.254.1    192.169.254.100  HTTP  1281 HTTP/1.1 200 OK  (text/html)
  13… 31.761651 192.169.254.100  192.169.254.1    HTTP   525 GET /favicon.ico HTTP/1.1
  13… 31.812189 192.169.254.1    192.169.254.100  HTTP  1281 HTTP/1.1 200 OK  (text/html)
  15… 46.950717 192.169.254.100  192.169.254.1    HTTP   165 GET /connecttest.txt HTTP/1.1
  15… 46.955770 192.169.254.1    192.169.254.100  HTTP   228 HTTP/1.1 307 Temporary Redirect

Frame 7: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits)

Hypertext Transfer Protocol: Protocol    Packets: 1763 · Displayed: 46 (2.6%)    Profile: Default
```

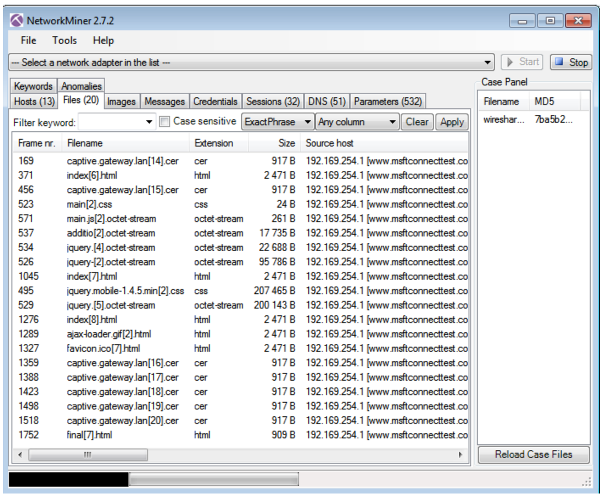
Figure 11 . Monitoring Results on HTTP Protocol

Figure 11 shows the HTTP filter HTTP protocol traffic on the Wireshark application. The HTTP protocol is a website component that regulates data exchange that occurs on the Internet. The way it works is that this protocol allows the web client (browser) and web server (web application) to communicate with each other connected. Seen that IP 192.169.254.100 did request IP 192.169.254.1. then IP

192.169.254.100 is directed to access the site that was deliberately created by the attacker. In the HTTP protocol, you can see several files suspicious like HTML and CSS files**.**

4.5. Disposition

Disposition is the final stage of research that is securing evidence obtained from the results of monitoring attacks and analyzing differences between real and fake wifi. With the disposition, the investigator can recapitulate all the data you want to get.



Frame nr.	Filename	Extension	Size	Source host
169	captive.gateway.lan[14].cer	cer	917 B	192.169.254.1 [www.msftconnecttest.co
371	index[6].html	html	2 471 B	192.169.254.1 [www.msftconnecttest.co
456	captive.gateway.lan[15].cer	cer	917 B	192.169.254.1 [www.msftconnecttest.co
523	main[2].css	css	24 B	192.169.254.1 [www.msftconnecttest.co
571	main.js[2].octet-stream	octet-stream	261 B	192.169.254.1 [www.msftconnecttest.co
537	additio[2].octet-stream	octet-stream	17 735 B	192.169.254.1 [www.msftconnecttest.co
534	jquery.[4].octet-stream	octet-stream	22 688 B	192.169.254.1 [www.msftconnecttest.co
526	jquery-[2].octet-stream	octet-stream	95 786 B	192.169.254.1 [www.msftconnecttest.co
1045	index[7].html	html	2 471 B	192.169.254.1 [www.msftconnecttest.co
495	jquery.mobile-1.4.5.min[2].css	css	207 465 B	192.169.254.1 [www.msftconnecttest.co
529	jquery.[5].octet-stream	octet-stream	200 143 B	192.169.254.1 [www.msftconnecttest.co
1276	index[8].html	html	2 471 B	192.169.254.1 [www.msftconnecttest.co
1289	ajax-loader.gif[2].html	html	2 471 B	192.169.254.1 [www.msftconnecttest.co
1327	favicon.ico[7].html	html	2 471 B	192.169.254.1 [www.msftconnecttest.co
1359	captive.gateway.lan[16].cer	cer	917 B	192.169.254.1 [www.msftconnecttest.co
1388	captive.gateway.lan[17].cer	cer	917 B	192.169.254.1 [www.msftconnecttest.co
1423	captive.gateway.lan[18].cer	cer	917 B	192.169.254.1 [www.msftconnecttest.co
1498	captive.gateway.lan[19].cer	cer	917 B	192.169.254.1 [www.msftconnecttest.co
1518	captive.gateway.lan[20].cer	cer	917 B	192.169.254.1 [www.msftconnecttest.co
1752	final[7].html	html	909 B	192.169.254.1 [www.msftconnecttest.co

Filename	MD5
wireshar...	7ba5b2...

Figure 12. Data File Result from Monitoring Wireshark

In Figure 12 found several suspicious files such as HTML and CSS files. The index.html file contains the login page code which was made intentionally by the perpetrators sourced from the IP 192.169.254.1 and also the main.css file, which isa file for custom layout on the login page which is also intentionally created with the same source IP as the HTML file. From this analysis, it can be concluded that the assailant attempted to deceive the victim by creating the same wifi asthe original wifi and redirecting the victim forcibly to the loginpage to input the password**.**

Table 3. Results of Wifi Analysis

No	SSID	BSSID	Vendor	Hostname
1	431 SQUARD	C4:B8:B4:8C:60:40	HUAWEI TECHNOLOGIES CO.,LTD	captive.gateway.lan, edge.microsoft.com, www.msftconnecttest.com
2	431 SQUARD	C4:B8:B4:8C:6F:40	HUAWEI TECHNOLOGIES CO.,LTD	-

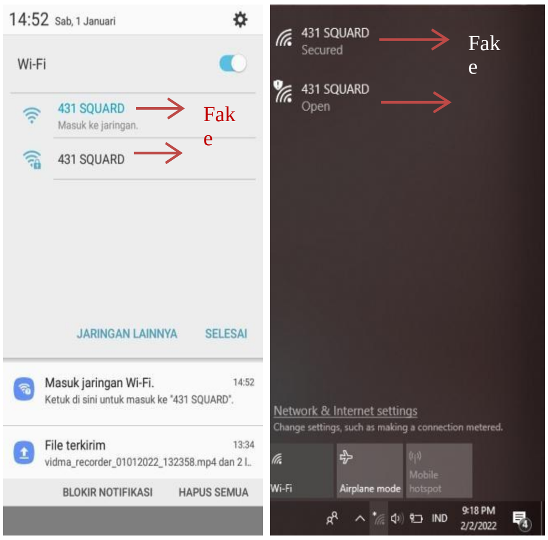
Table 3 is the result of monitoring which is seen information from real and fake wifi. The difference that can be seen is in BSSID and Hostname, where for wifi the first is fake wifi with BSSID C4:B8:B4:8C:60:40 and has various hostnames. And for the second wifi is original with a difference on BSSID that is C4:B8:B4:8C:6F:40 and has no hostname.

Tabel 4. Pcap File Analysis Results

Time	Source	Destination	Length	Info
ARP Protocol Analysis				
01-01-2022 (17:14)	HuaweiTe_8c:60:40	Broadcast	42	Who has 192.169.254.100? tell 192.169.254.1
	2a:bf:ff:19:78:49	HuaweiTe_8c:60:40	42	192.169.254.100 is at 2a:bf:ff:19:78:49
	2a:bf:ff:19:78:49	Broadcast	42	Who has 192.169.254.100 ? (ARP Probe)
HTTP Protocol Analysis				
01-01-2022 (17:14)	192.169.254.100	192.169.254.1	165	GET /connecttest.txt HTTP/1.1
	192.169.254.100	192.169.254.1	510	GET /redirect HTTP/1.1
	192.169.254.100	192.169.254.1	577	GET / HTTP/1.1
01-01-2022 (17:15)	192.169.254.100	192.169.254.1	165	GET /connecttest.txt HTTP/1.1
	192.169.254.100	192.169.254.1	165	GET /connecttest.txt HTTP/1.1
	192.169.254.100	192.169.254.1	510	GET /css/jquery.mobile-1.4.5.min.css HTTP/1.1
	192.169.254.100	192.169.254.1	491	GET /css/main.css HTTP/1.1
	192.169.254.100	192.169.254.1	408	GET /js/jquery-1.11.1.min.js HTTP/1.1
	192.169.254.100	192.169.254.1	414	GET /js/jquery.mobile-1.4.5.min.css HTTP/1.1
	192.169.254.100	192.169.254.1	410	GET /js/jquery.validate.min.js HTTP/1.1
	192.169.254.100	192.169.254.1	413	GET /js/additional-methods.min.js HTTP/1.1
	192.169.254.100	192.169.254.1	395	GET /js/main.js HTTP/1.1
	192.169.254.100	192.169.254.1	571	GET /css/images/ajax-loader-gif HTTP/1.1
	192.169.254.100	192.169.254.1	525	GET /favicon.ico HTTP/1.1
	192.169.254.100	192.169.254.1	165	GET /connecttest.txt HTTP/1.1
	192.169.254.100	192.169.254.1	600	POST /check.php HTTP/1.1
	192.169.254.100	192.169.254.1	527	GET /final.html HTTP/1.1
File Identification Analysis				
01-01-2022 (17:14)	192.169.254.1	192.169.254.100	1281	HTTP/1.1 200 OK (text/html)
01-01-2022 (17:15)	192.169.254.1	192.169.254.100	291	HTTP/1.1 200 OK (text/css)
	192.169.254.1	192.169.254.100	1281	HTTP/1.1 200 OK (text/html)
	192.169.254.1	192.169.254.100	414	HTTP/1.1 200 OK (text/css)
	192.169.254.1	192.169.254.100	1281	HTTP/1.1 200 OK (text/html)
	192.169.254.1	192.169.254.100	1281	HTTP/1.1 200 OK (text/html)
	192.169.254.1	192.169.254.100	1281	HTTP/1.1 200 OK (text/html)

Table 4 is the result of the analysis of the monitoring that has been carried out where the results of the analysis are divided into 3 hierarchies, namely HTTP Protocol, Protocol ARP, and Media Presentation Protocol. The results of the analysis on the ARP protocol which was conducted on January 1, 2022, At 5:14 PM, that Mac Address of 2a:bf:ff:19:78:49 with IP Address

192.169.254.100 tried contacting MAC Address Destination HuaweiTe_8c:60:40 with IP 192.169.254.1. In the HTTP protocol there are 2 methods for activities done by the victim, namely, GET to call or display a request and POST to send data that has been inputted. On IP 192.169.254.100 made several requests to IP 192.169.254.1. And for file identificationanalysis here IP 192.169.254.1 receives a request and sends it to IP 192.169.254.100 by displaying the layout from created HTML and CSS files



(a) (b)

Figure 13. Real and Fake Wifi

After analyzing the results of monitoring then analyze the difference between real and fake wifi. Figure 13(a) displays wifi that has the same SSID on a mobile device. Todistinguish it, the original wifi has a padlock mark which means when youwant to access it, the user inputs the password first, while the fake wifi does not have a sign that means it does not have security. Figure 13(b) is an example of a laptop device with windows 10 OS. The difference in fake wifi says Open and hasan exclamation point which means the wifi has no security, for the original wifi that says Secured.

5. CONCLUSION

Based on the results of tests that have been conducted using the Network Forensics Development Life Cycle (NFDLC) method,it can be concluded that investigative analysis using the Network Forensics Development Life Cycle (NFDLC) method, produces several complete analyses with various stages of Initiations, Acquisition, Implementation, Operations, and Disposition. The results of the investigation analyzed the equipment used in attack activities, then the installation of tools, the flowchart of investigations and attacks, simulation of attacks, analysis of monitoring results, and analysis of differences between real wifi and fake wifi. Based on the results of monitoring analyzed from 3 hierarchies namely

Protocol ARP, PROTOCOL HTTP and Media Presentation Protocol concluded that from the traffic flow there are some suspicious communications from interactions that contain an HTML and CSS file with illegal and aim to force the victim to enter wifipassword data into a website. This action is different from what is done if you access the original wifi.

6. REFERENCES

[1] Ahmad, M. S., Riadi, I., & Prayudi, Y. (2017). LiveForensic Investigation From User Side To Analyze Evil Twin-Based Man in the Middle Attack. ILKOM Scientific Journal, 9(1), 1–8.

[2] Salman, O., Elhajj, I. H., Chehab, A., & Kayssi, A. (2018). A Multi-level Internet Traffic Classifier Using Deep Learning. 2018 9th International Conference on theNetwork of the Future (NOF), 68–75.

[3] Aji, S., Fadlil, A., & Riadi, I. (2017). Development of a Computer Network Security System Based on Network Forensic Analysis. Scientific Journal of Computer and Informatics Electrical Engineering, 3(1), 1.

[4] Vishwa Modi, & Asst. Prof. Chandresh Parekh. (2017). Detection of Rogue Access Point to Prevent Evil Twin Attack in Wireless Network. International Journal of Engineering Research And, V6(04), 23–26.

[5] S. Ayare, S. Das, V. Sayanekar, dan P. R. Patkar. (2010) "Fake access point detection in network," Int. J. Adv. Res. Comput. Commun.

[6] Paramita, F., Alvina, O., Sentia, R. E., & Kurniawan, A. (2021). Unauthorized Access Point Analysis UsingNetwork Forensics Techniques. Telematics Journal, 14(2), 10.

[7] Singh, O., (2009). Network Forensics. Indian Computer Response Team (CERT- In) Department of Information Technology, New Delhi, India.

[8] Putri, R. U., & Istiyanto, J. E. (2013). Network Forensic Analysis Case Study SQL Injection Attack on Gadjah Mada University Server. IJCCS (Indonesian Journal of Computing andCybernetics Systems), 7(1).

[9] Sulianta, F., (2008), Forensic Computer Jakarta : PT.Elex Media Komputindo

[10] I. Riadi dan A. Kurniawan. (2019). Forensic Network & Cloud. yogyakarta: DiandraKreatif.

[11] Tella, F., Riadi, I. (2020). Comparison of Network Forensics Results Against E-mail Spamming and Spoofing Attacks. XII (2), 121–127.

[12] Hermaduanti, N. (2016). Development of Mitigation Framework for Mitigation of Rogue Access Point Cases on Ieee 802.1X Wireless Networks.

[13] Zamidra zam, E. (2014). Easy Ways to Create a Wireless Network. Elex Media Komputindo.

[14] Sari, M. W. (2016). Analysis of Wi-Fi Network Security Using the Signal Scanning Method at the Faculty of Engineering, Pgri Yogyakarta University. Yogyakata.

[15] University, S., Mada, G., & Mada, G. (2013). Network Forensic Analysis CaseStudy of SQL Injection Attack on Gadjah Mada University Server. IJCCS (Indonesian Journal of Computing andCybernetics Systems), 6(2).

[16] M. Agarwal, S. Biswas, and S. Nandi. (2018). An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi- Fi Networks, International Journal of Wireless Information Networks, pp. 1-16.

[17] Z. Tang, Y. Zhao, L. Yang, S. Qi, D. Fang, X. Chen, et al. (2017). Exploiting wireless received signal strength indicators to detect evil- twin attacks in smart homes. Mobile Information Systems, vol. 2017.

[18] Alsahlany, A. M., Almusawy, A. R., & Alfatlawy, Z. H. (2018). Risk analysis of afake access point attack against Wi-Fi network. 9(5), 322–326.

[19] A. Kumar dan P. Paul. (2016). Security analysis and implementation of asimple method for prevention and detection against evil twin attackin IEEE 802.11 wireless LAN. International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT).

[20] Lasaharu, S., & Riadi, I. (2022). Network Forensic on Web-based Applications using Network Forensic Development Life Cycle Method. International Journal of Computer Applications, 183(47), 8–14.

[21] Hidayat, M. R., & Riadi, I. (2021). Investigation of Botnet Attacks using Network Forensic Development Life Cycle Method. International Journal of Computer Applications, 183(25), 30–36.

[22] Pratama, I. P. A. E. (2014). Computer Networking (1st ed.). Bandung: Bandung Informatics.

[23] Purba, W. W., & Efendi, R. (2021). Design and analysis of computer network security systems using SNORT. Aiti, 17(2), 143–158.

[24] Rahmatulloh, A., & MSN, F. (2017). Implementation of Load Balancing Web Server using proxy and File Synchronization on the AcademicInformation System of Siliwangi University. National Journal of Information Technology and Systems, 3(2), 241–248.

[25] Sudradjat, B. (2017). Intruder Detection and Prevention System On Computer Networks Using Snort and Firewalls. JISAMAR (Journal of Information Systems, Applied, Management, Accounting and Research), 1(1), 10–24.