FORENSICS ANALYSIS OF OPEN WIFI NETWORK

Reesha P[1], Elizabeth Rose Lalson[2]

Student, Dept. of Computer Science, ER & DCI Institute of Technology, Trivandrum, Kerala, India
Assistant Professor, ER & DCI Institute of Technology, Trivandrum, Kerala, India

---***---

Abstract - *Wi-Fi (wireless fidelity) based on IEEE 802.11 standards is a family of radio technologies commonly used for wireless local area networking (WLAN) of devices. Nowadays most of the Smartphone/mobile phone owners use public Wi-Fi hotspots. But there are many security risks associated while accessing this open Wi-Fi network. All data sent over an unsecured wireless network, one that doesn't require a Wi-Fi Protected Access (WPA) or WPA2 password is sent in plain content for anyone to catch. The ease in availability of open Wi-Fi network, increased the number of criminal activities using open Wi-Fi. Therefore the forensic analysis of open Wi-Fi network is very important. This paper discuss about forensic analysis of open Wi-Fi Network by capturing network traffic and analysing the captured traffic the system extracts the forensics evidences including source and destination of packets, URLs, ports, Malicious users, unwanted websites visited its frequency etc. The proposed system also detects the two most common attacks in open Wi-Fi such as DoS and Evil Twin attack.*

Key Words: **Wireless Fidelity, Open Wi-Fi, Wireless Protected Access, Access Point, DoS Attack, Evil Twin Attack.**

1. INTRODUCTION

Wireless Fidelity (Wi-Fi) is a way of getting high speed internet service to a gadget or device using wireless transmitters and radio frequency signals. When a transmitter gets information from the internet, it changes over the information into a radio frequency signal that can be gotten and perused by Wi-Fi empowered devices. Then data is swapping between the transmitter and the device.

The existing security mechanisms available in the Wi-Fi network are WEP, WPA, and WPA2. These wireless security protocols prevent unauthorized access to your wireless network and also encrypt the data sent over the network. WEP (Wired Equivalent Privacy) is the first of Wireless Security Protocols, developed in 1999. It was aimed to protect the wireless data between clients and access points. But the cyber security experts detected many vulnerabilities in this wireless security protocol [1]. Wi-Fi Protected Access (WPA) was developed in 2003 by Wi-Fi Alliance. WPA is using 256-bit WPA-PSK (Pre-Shared Key) [2]. With WPA two new security components such as "Message Integrity Check" and "Temporal Key Integrity Protocol (TKIP)" are introduced. These mechanism makes the transmission of data more secure and ensured the integrity of the data. WPA2 (Wi-Fi Protected Access 2) [2] has developed in 2006 and it was a propelled version of WPA. WPA2 gave new encryption and authentication mechanisms to provide more secure networks. These mechanisms include AES (Advanced Encryption Standard) and CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol). So currently this is the commonly used security mechanism in Wi-Fi. In simple terms this protocol requires an unique password to be entered by the user before accessing the internet using Wi-Fi which ensures the security in Wi-Fi.

Nowadays most of the mobile device and laptop users use open Wi-Fi network or public Wi-Fi hotspot in many places like in restaurants, hotels, railway stations, airports etc may be due to the unavailability of our own network or to get higher bandwidth internet. There are usually two types of open Wi-Fi networks secured and unsecured. In secured open Wi-Fi the users have to complete a registration process and also have to enter the password got during registration before accessing the internet. But in unsecured open Wi-Fi any user can freely access the internet, even without entering any password. Usually the users prefer to use the second kind of open Wi-Fi for their convenience and ease of use. All information sent over an unsecured wireless network, one that doesn't require a Wi-Fi Protected Access (WPA) or WPA2 password is despatched in plain content for everybody to intercept. So in this kind of open Wi-Fi, the data sent over public Wi-Fi network can be easily grabbed and users are putting their own data at high risk. Connecting to an open network probably opens your machine to every person else on that same Wi-Fi network. When signing in to a website or using a utility that sends information in clear text over a network anyone in close proximity can easily capture that information.

In this paper we are discussing about the various security issues in open Wi-Fi, the most common attacks and how we can perform a forensic analysis in open Wi-Fi network. The forensics process involves capturing all data moving over the network and analyzing network events in order to discover the source and destination information, URLs visited and detects two most common attacks such as DoS and evil twin attack. The forensic tool will also be capable of searching for the suspicious users of an access point and if a suspicious user is found using this tool there is also option in this tool to search for the urls he/she visited.

2. SECURITY ISSUES IN OPEN WI-FI

In open Wi-Fi systems, you are interfacing with a system without knowing who is setting up that system or who else should be on the system. Free Wi-Fi gave by bistros, cafés, and so forth fills in as brilliant spots for gathering passwords. The attacker can launch the MITM attack by deploying ARP Cache Poisoning and can peruse all passwords in plaintext (Email not utilizing TLS), sites without SSL, user's google searches, and so forth. A more advanced attacker may set up a functioning intermediary to lead assaults, for example, SSL Stripping on his PC, which would give him access to all the destinations you visit, including HTTPS. That means he now has passwords for your PayPal, Facebook, and Twitter. So there is a high chance to misuse the Wi-Fi network for criminal activity or a cyber attack.

The two most common basic public Wi-Fi network attacks which we are discussing in this paper are DoS attack and Evil twin attack. A Denial-of-Service (DoS) attack is an attack meant to shut down a system or network, denying the service to its intended users. DoS attacks can be performed by flooding the target device with traffic or sending it information to crash. In both scenarios, the DoS attack denies the service of legitimate users. Flood attacks occur when the victim or system receives too much traffic for the server to buffer, causing them to slow down and inevitably stop. Other DoS attacks exploit vulnerabilities that will lead the target system or service to crash. DoS attacks can be of different types[3] Physical layer DoS attacks such as tampering, Jamming etc, Data Link Layer Dos attacks such as Collision, Exhaustion through Network Injection etc, Network Layer Dos Attacks such as IP Spoofing, Smurf Attack etc and Transport Layer Dos attacks such as TCP Flooding, UDP Flooding, DeSynchronization etc.

Another most common and dangerous Wi-Fi attack is an evil twin attack. DoS attack and Evil Twin attack are closely interrelated too. In a normal Wi-Fi network, a client device associates with a legitimate access point (AP). In an evil twin attack, the attacker creates a rogue AP with same SSID (name of AP) and BSSID (MAC address of AP) of the legitimate AP. In some cases they fakes only SSID. So the normal/genuine STAs(stations) will be tricked to connect with the Rogue AP rather than Legitimate AP. Regularly, the victims of such attacks are normal people since they try to connect to an AP with stronger signal strength and that will be usually satisfied by rogue APs. If the option to automatically connect to the AP is enabled in some genuine STAs, all these STAs will be connected to this Rogue AP since it has the same SSID as that of legitimate APs and more signal strength. The fake Wi-Fi access point can then be used to listen to users and steal their login credentials or other sensitive information. In some cases rogue APs spoof only SSID of legitimate APs where in some others they spoof both SSID and BSSID. Also after launching the attack to provide internet to the STAs the attacker in some cases use their own network or they connect to legitimate AP for providing internet, in the later they act as a man in the middle.

3. RELATED WORK

Nadia Benchikha, Mohamed Krim, et al [4] proposed an integrated framework "IWNetFAF"- An Integrated Wireless Network Forensic Analysis Framework that captures and analyzes 802.11 wireless network traffic to identify attacks and malicious behaviors. Three attacks detected using this framework were WEP crack attack, DoS attack and Evil Twin attack. The attack detections were based on attack signature such as number of deauthentication frames, gap in sequence numbers etc. Niharika Sharma, Amit Mahajan, Vibhakar Mansotra [5] proposed a framework to capture data in the form of PCAP file to study and analyze the Dos SYN flood attacks using decision tree data mining tool. In [6] Parekh proposed a solution to detect Evil Twin Attack. Here two scenarios of Evil Twin Attack is proposed and also this paper discuss with the possible evidences left behind in the above scenarios to detect evil twin attack.

4. PROPOSED SYSTEM

The purpose of the proposed tool is to perform forensic analysis of open Wi-Fi network traffic. The background study conducted revealed that there is a need to develop a more efficient forensic tool which analyse the network dump, gather forensic evidences and also detect the attacks. It should also trace the source of attack. The proposed system analyzes the captured data moving over the network and provides a complete forensic report which includes forensic information such as:

- Source IP and destination IP address of packets
- URLs visited by the user
- Devices which visited a particular URL
- DoS Attack Detection and its source
- Evil Twin Attack Detection and its source

Fig 1 shows the system architecture of the proposed system. Upper layer is the user interface layer and the lower layer consists of sub modules packet capturing, packet analysis and report generation.

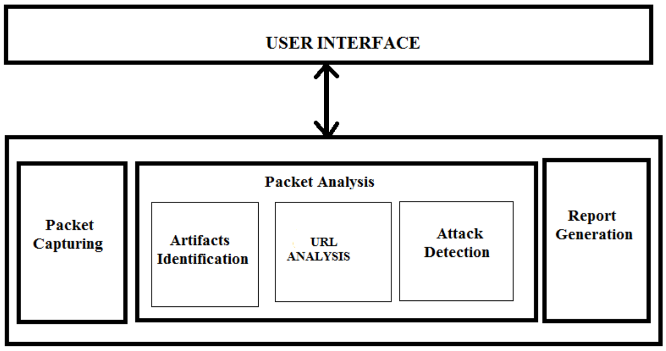


Fig-1: System Architecture

Packet capturing module captures the packets moving over the network. Network traffic capturing can be done by using a third-party tool and gives the captured packets as input for the analysis module. The analysis module analyse the headers of the packet and extract key artefacts which may include IP address, MAC Address, Port Number, and the Protocol type. This Information will be displayed in a table as output of header details.

In the analysis module the system also performs the url analysis, here a table will be generated which will consists of the top websites visited by user. Since there might be numerous packets with a similar source ip address and destination ip address which have distinctive timestamps and bundle types, this will assist the investigator for identifying suspicious hosts. Also if an investigator enters a particular url or ip address, the system will detect whether any user accessed that url or ip address and if yes how often the system accessed that url.

In the attack analysis module two most common attacks in open Wi-Fi such as DoS and Evil Twin attacks are also detected. In the proposed system, for implementation purpose the DoS attack is performed by broadcasting SYN packets .The target machine responds to each one of the connection requests and leaves an open port ready to receive the response. While the target machine waits for the final ACK packet, which never arrives, the attacker continues to send more SYN packets. The arrival of each new SYN packet causes the target machine to temporarily maintain a new open port connection for a certain length of time, and once all the available ports have been utilized the target machine is unable to function normally. If the number of SYN packets is greater than threshold value, then we can conclude that the attacker aims launching a DoS attack. For the study purpose we have confined the study to SYN flood DoS attack detection which can be extended further to find all kinds of DoS attacks.

The Evil Twin attack as discussed earlier consists of creating a rogue AP by spoofing Service Set Identifier (SSID) of the legitimate AP. The rogue AP tricks victim STAs or client devices into connecting to it by sending deauthentication frames. So to detect Evil twin attacks one thing we can use is to check the dump file for the existence of consequent deauthentication frames sent by legitimate AP. Detecting such deauthentication frames from particular BSSID indicating a possible Evil Twin Attack. If same SSIDs are having two different BSSID it can also be considered as a strong evidence for identifying the evil twin attack.

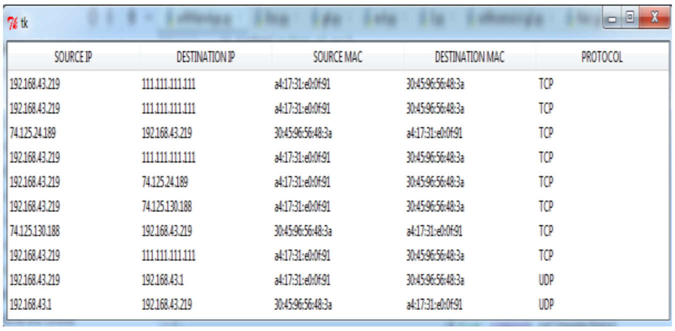
5. IMPLEMENTATION AND RESULTS

5.1 Packet Capturing

The network traffic is captured using wireshark and the output is a dump file with an extension of .pcap.

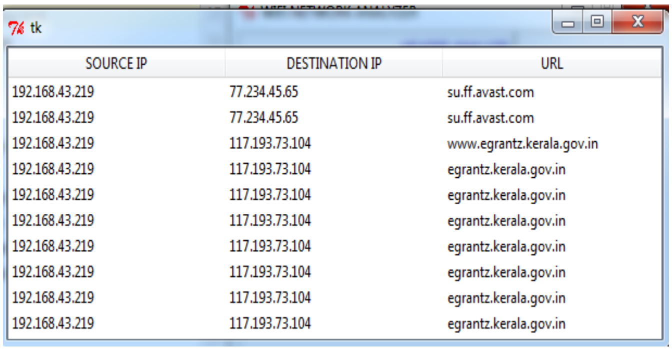
5.2 Header Analysis & URL Analysis

Fig 2 shows header details of the packets extracted from the dump file and Figure 3 shows the result of URL analysis.



SOURCE IP	DESTINATION IP	SOURCE MAC	DESTINATION MAC	PROTOCOL
192.168.43.219	111.111.111.111	a4:17:31:e0:0f:91	30:45:96:56:48:3a	TCP
192.168.43.219	111.111.111.111	a4:17:31:e0:0f:91	30:45:96:56:48:3a	TCP
74.125.24.189	192.168.43.219	30:45:96:56:48:3a	a4:17:31:e0:0f:91	TCP
192.168.43.219	111.111.111.111	a4:17:31:e0:0f:91	30:45:96:56:48:3a	TCP
192.168.43.219	74.125.24.189	a4:17:31:e0:0f:91	30:45:96:56:48:3a	TCP
192.168.43.219	74.125.130.188	a4:17:31:e0:0f:91	30:45:96:56:48:3a	TCP
74.125.130.188	192.168.43.219	30:45:96:56:48:3a	a4:17:31:e0:0f:91	TCP
192.168.43.219	111.111.111.111	a4:17:31:e0:0f:91	30:45:96:56:48:3a	TCP
192.168.43.219	192.168.43.1	a4:17:31:e0:0f:91	30:45:96:56:48:3a	UDP
192.168.43.1	192.168.43.219	30:45:96:56:48:3a	a4:17:31:e0:0f:91	UDP

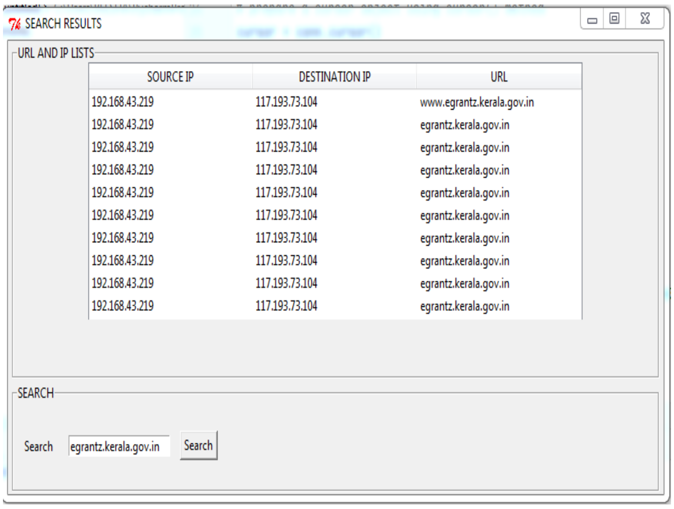
Fig-2: Header Details



SOURCE IP	DESTINATION IP	URL
192.168.43.219	77.234.45.65	su.ff.avast.com
192.168.43.219	77.234.45.65	su.ff.avast.com
192.168.43.219	117.193.73.104	www.egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in

Fig-3: URL Details

Figure 4 shows search result which is used to check whether the user has visited a particular url. Table consists of source and destination IP address and the url visited by the user.

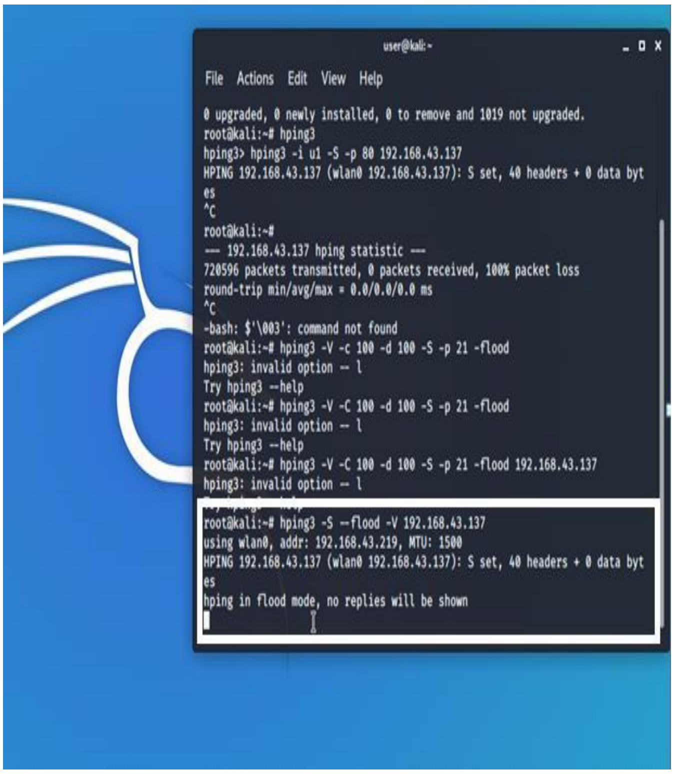


SOURCE IP	DESTINATION IP	URL
192.168.43.219	117.193.73.104	www.egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in
192.168.43.219	117.193.73.104	egrantz.kerala.gov.in

Fig-4: Search result for URL input

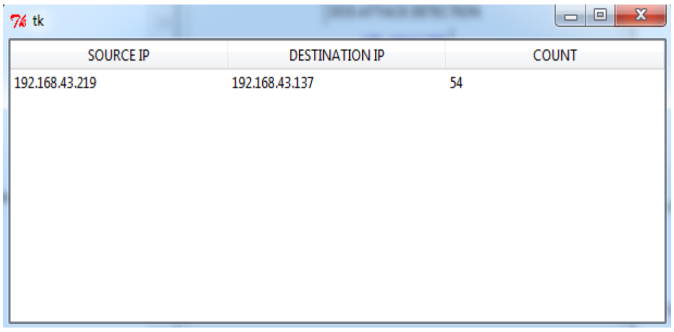
5.3 DoS Attack Detection

DoS Attack was performed Using the tool Hping3 in kali Linux. Performed TCP-SYN Flood attack on the target device 192.168.43.137. Figure 5 shows screenshot of command used for performing DoS (TP-SYN flood) attack. Figure 6 shows details of DoS attack. In the alert message when click on OK Button details such as source and destination IP address and count of SYN packets will display on a new window.



```
0 upgraded, 0 newly installed, 0 to remove and 1019 not upgraded.
root@kali:~# hping3
hping3> hping3 -i u1 -S -p 80 192.168.43.137
HPING 192.168.43.137 (wlan0 192.168.43.137): S set, 40 headers + 0 data byt
es
^C
root@kali:~#
--- 192.168.43.137 hping statistic ---
720596 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
^C
-bash: $'\003': command not found
root@kali:~# hping3 -V -c 100 -d 100 -S -p 21 -flood
hping3: invalid option -- l
Try hping3 --help
root@kali:~# hping3 -V -C 100 -d 100 -S -p 21 -flood
hping3: invalid option -- l
Try hping3 --help
root@kali:~# hping3 -V -C 100 -d 100 -S -p 21 -flood 192.168.43.137
hping3: invalid option -- l
root@kali:~# hping3 -S --flood -V 192.168.43.137
using wlan0, addr: 192.168.43.219, MTU: 1500
HPING 192.168.43.137 (wlan0 192.168.43.137): S set, 40 headers + 0 data byt
es
hping in flood mode, no replies will be shown
```

Fig-5: DoS Attack

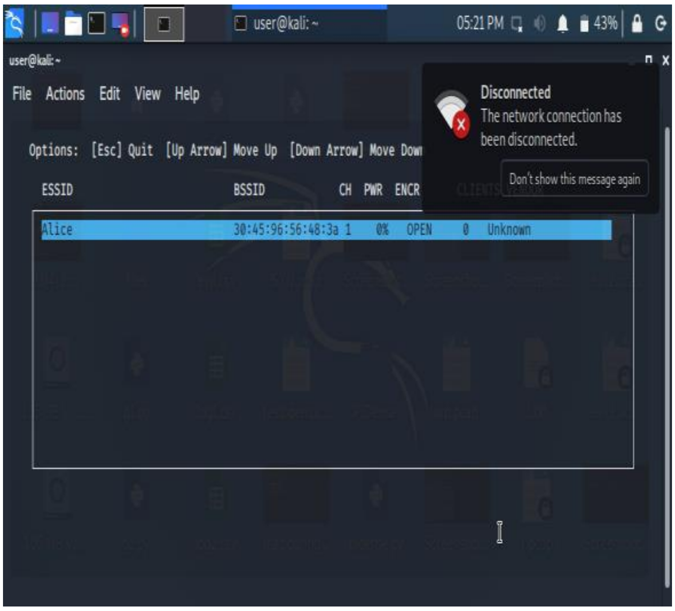


SOURCE IP	DESTINATION IP	COUNT
192.168.43.219	192.168.43.137	54

Fig-6: DoS Attack Details

5.4 Evil Twin Attack Detection

Evil twin attack was performed using a third party tool wifiphisher. Attack was performed using kali Linux machine. Initially a client device named realme-5 with BSSID 58:85:a2:f1:12:17 connected with the legitimate AP having SSID '**Alice**' and BSSID 30:45:96:56:48:3A. The attacker machine (Kali Linux) launches the evil twin attack with wifiphisher tool. Now this tool scans all the available Wi-Fi networks by putting the network interface card into monitor mode. Figure 7 shows available Wi-Fi networks listed by wifiphisher tool.

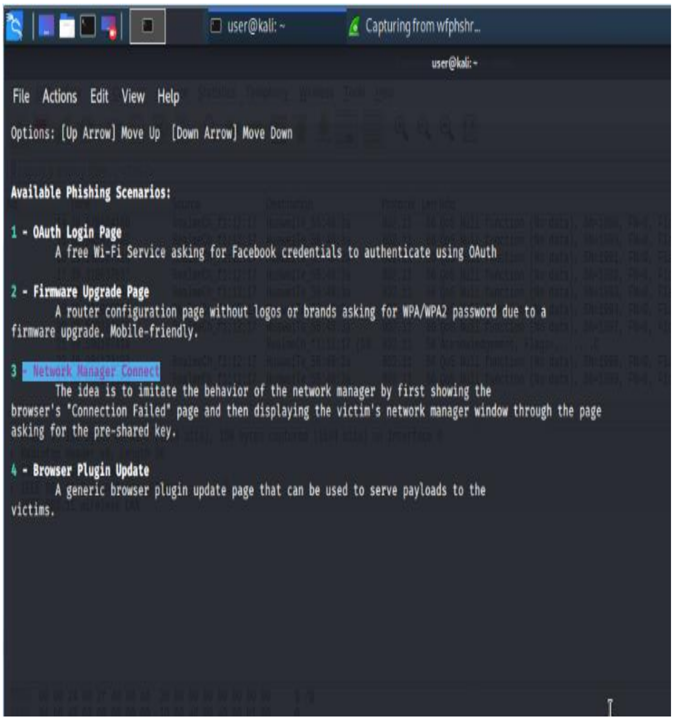


Disconnected
The network connection has been disconnected.

```
Options:  [Esc] Quit  [Up Arrow] Move Up  [Down Arrow] Move Dow

  ESSID                BSSID             CH  PWR  ENCR

 Alice                 30:45:96:56:48:3a 1    0%   OPEN    0   Unknown
```

Fig-7: Wifiphisher tool lists all the available Wi-Fi networks

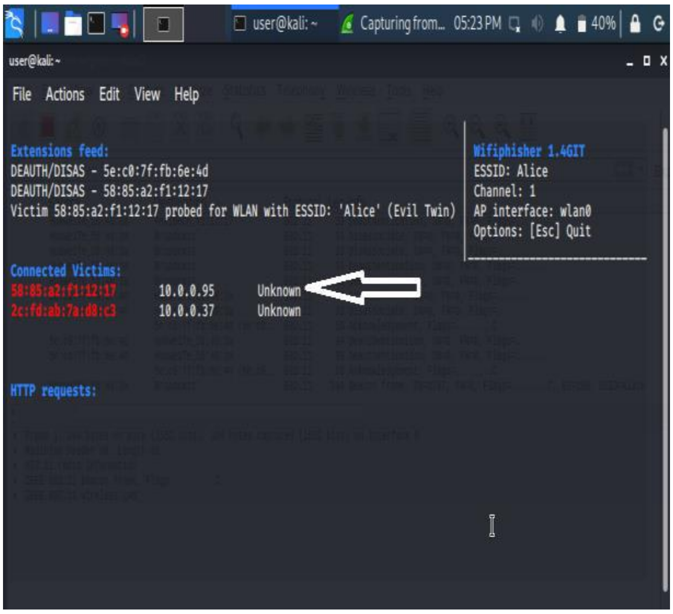
Now start the packet capturing tool wireshark in monitor mode in-order to capture the packets. Attacker selects the Wi-Fi network from the displayed list. Now the tool shows some attack method options. For launching evil twin attack select Network Manager Connect option. Figure 8 shows attacker machine selecting the option Network Manager connect option to launch the attack.



```
Options: [Up Arrow] Move Up  [Down Arrow] Move Down

Available Phishing Scenarios:

1 - OAuth Login Page
        A free Wi-Fi Service asking for Facebook credentials to authenticate using OAuth

2 - Firmware Upgrade Page
        A router configuration page without logos or brands asking for WPA/WPA2 password due to a
firmware upgrade. Mobile-friendly.

3 - Network Manager Connect
        The idea is to imitate the behavior of the network manager by first showing the
browser's "Connection Failed" page and then displaying the victim's network manager window through the page
asking for the pre-shared key.

4 - Browser Plugin Update
        A generic browser plugin update page that can be used to serve payloads to the
victims.
```

Fig-8: Selecting attack method Network Manager Connect option

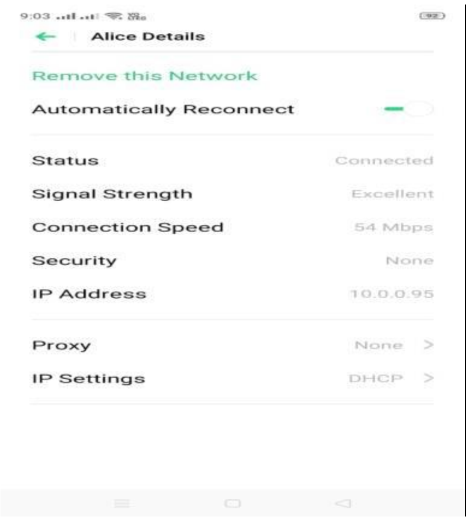
After selecting the attack method, wifiphisher tool starts the attack by creating the rogue access point with same SSID as legit AP. The tool then sends deauthentication frames to disconnect the clients from the legit AP and to connect to the rogue AP. Now on the attacker machine it shows that client device is connected to the rogue access point. Figure 9 shows client device is connected to the rogue AP having SSID 'Alice'.



```
Extensions feed:                                                   Wifiphisher 1.4GIT
DEAUTH/DISAS - 5e:c0:7f:fb:6e:4d                                   ESSID: Alice
DEAUTH/DISAS - 58:85:a2:f1:12:17                                   Channel: 1
Victim 58:85:a2:f1:12:17 probed for WLAN with ESSID: 'Alice' (Evil Twin)   AP interface: wlan0
                                                                   Options: [Esc] Quit

Connected Victims:
58:85:a2:f1:12:17      10.0.0.95      Unknown
2c:fd:ab:7a:d8:c3      10.0.0.37      Unknown

HTTP requests:
```

Fig-9: client device is connected to the rogue access point

After the attack legit AP will show list of connected devices 0 because the client device is now connected to the rogue AP. Now the client device shows it is connected to rogue AP having the IP address 10.0.0.95 allotted by wifiphisher tool. Figure 10 shows the screenshot of the client device.

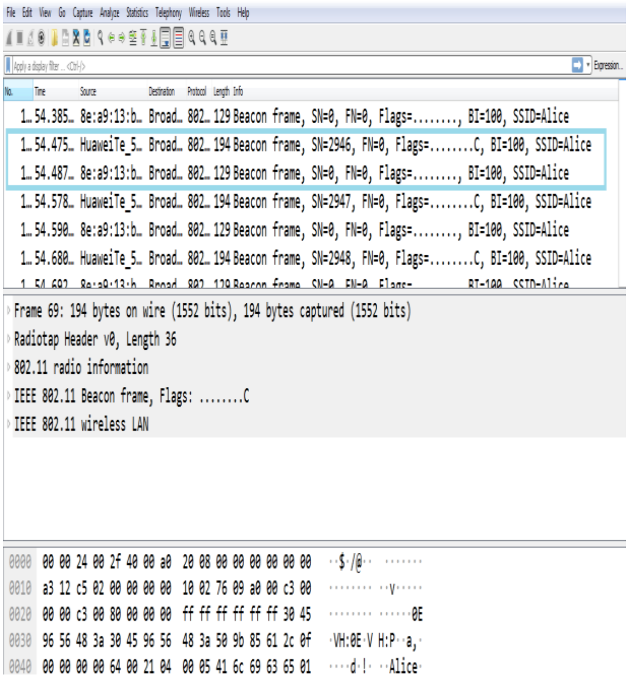


Alice Details

Status	Connected
Signal Strength	Excellent
Connection Speed	54 Mbps
Security	None
IP Address	10.0.0.95
Proxy	None >
IP Settings	DHCP >

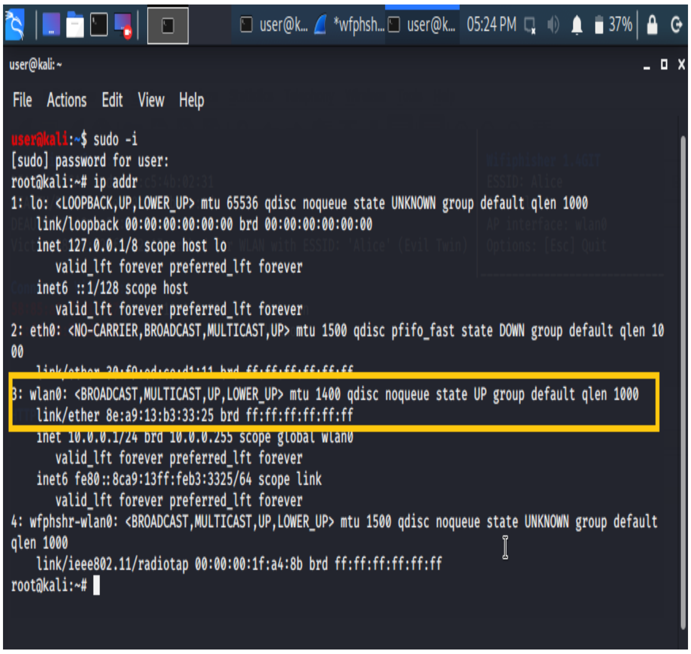
Fig-10: Client device after the attack is connected to the rogue AP

While analysing captured packet, two AP with same SSID but with different MAC address could be seen. So the same SSID with different MAC address indicates a possible evil twin attack. Figure 11 shows analysis of dump file. From dump file found SSID 'Alice' having different MAC address. In the dump file MAC address having same SSID as legit AP will be of attacker machine. But it is not static and will be changing for each time the attack launches. Figure 12 shows the MAC address details of the attacker machine during the attack.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

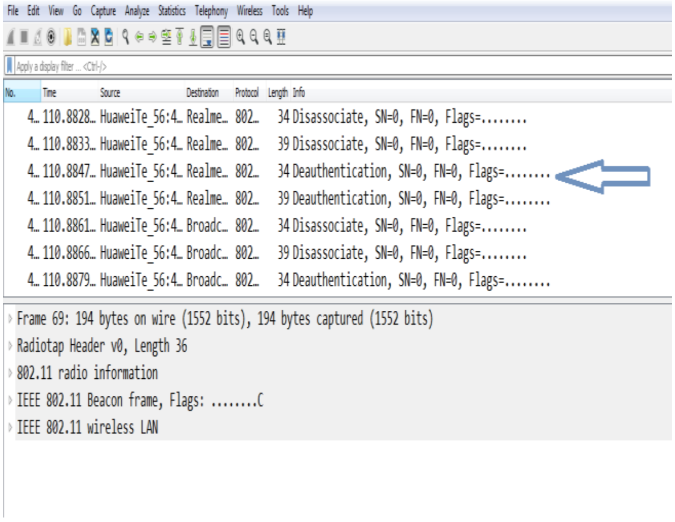
```
No.  Time      Source        Destination Protocol Length Info
1… 54.385… 8e:a9:13:b… Broad… 802… 129 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Alice
1… 54.475… HuaweiTe_5… Broad… 802… 194 Beacon frame, SN=2946, FN=0, Flags=........C, BI=100, SSID=Alice
1… 54.487… 8e:a9:13:b… Broad… 802… 129 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Alice
1… 54.578… HuaweiTe_5… Broad… 802… 194 Beacon frame, SN=2947, FN=0, Flags=........C, BI=100, SSID=Alice
1… 54.590… 8e:a9:13:b… Broad… 802… 129 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Alice
1… 54.680… HuaweiTe_5… Broad… 802… 194 Beacon frame, SN=2948, FN=0, Flags=........C, BI=100, SSID=Alice
1… 54.692… 8e:a9:13:b… Broad… 802… 129 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=Alice

Frame 69: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)
Radiotap Header v0, Length 36
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
IEEE 802.11 wireless LAN

0000  00 00 24 00 2f 40 00 a0  20 08 00 00 00 00 00 00   ··$·/@··  ········
0010  a3 12 c5 02 00 00 00 00  10 02 76 09 a0 00 c3 00   ········  ··v·····
0020  00 00 c3 00 80 00 00 00  ff ff ff ff ff ff 30 45   ········  ······0E
0030  96 56 48 3a 30 45 96 56  48 3a 50 9b 85 61 2c 0f   ·VH:0E·V  H:P··a,·
0040  00 00 00 00 64 00 21 04  00 05 41 6c 69 63 65 01   ····d·!·  ··Alice·
```

Fig-11: Same SSID with Different MAC address


user@k… *wfphsh… user@k… 05:24 PM 37%
user@kali: ~
File Actions Edit View Help

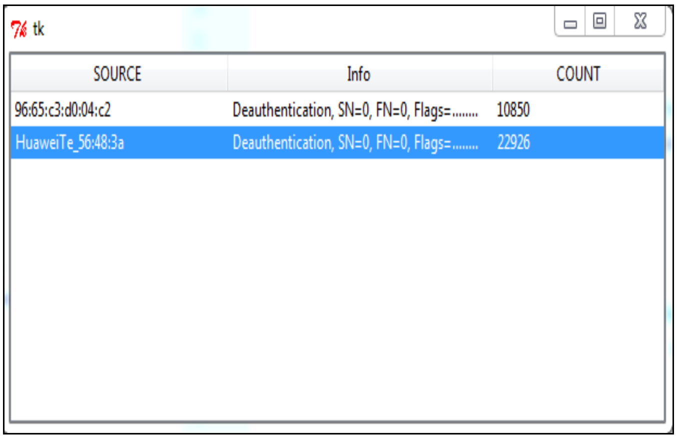
```
user@kali:~$ sudo -i
[sudo] password for user:
root@kali:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 10
00
    link/ether 30:f0:ed:ca:d1:11 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc noqueue state UP group default qlen 1000
    link/ether 8e:a9:13:b3:33:25 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/24 brd 10.0.0.255 scope global wlan0
       valid_lft forever preferred_lft forever
    inet6 fe80::8ca9:13ff:feb3:3325/64 scope link
       valid_lft forever preferred_lft forever
4: wfphshr-wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/ieee802.11/radiotap 00:00:00:1f:a4:8b brd ff:ff:ff:ff:ff:ff
root@kali:~#
```

Fig-12: MAC Address of Attacker Machine during the Attack


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time        Source            Destination Protocol Length Info
4… 110.8828… HuaweiTe_56:4… Realme… 802…  34 Disassociate, SN=0, FN=0, Flags=........
4… 110.8833… HuaweiTe_56:4… Realme… 802…  39 Disassociate, SN=0, FN=0, Flags=........
4… 110.8847… HuaweiTe_56:4… Realme… 802…  34 Deauthentication, SN=0, FN=0, Flags=........
4… 110.8851… HuaweiTe_56:4… Realme… 802…  39 Deauthentication, SN=0, FN=0, Flags=........
4… 110.8861… HuaweiTe_56:4… Broadc… 802…  34 Disassociate, SN=0, FN=0, Flags=........
4… 110.8866… HuaweiTe_56:4… Broadc… 802…  39 Disassociate, SN=0, FN=0, Flags=........
4… 110.8879… HuaweiTe_56:4… Broadc… 802…  34 Deauthentication, SN=0, FN=0, Flags=........

Frame 69: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)
Radiotap Header v0, Length 36
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
IEEE 802.11 wireless LAN
```

Fig-13: Deauthentication frames



SOURCE	Info	COUNT
96:65:c3:d0:04:c2	Deauthentication, SN=0, FN=0, Flags=........	10850
HuaweiTe_56:48:3a	Deauthentication, SN=0, FN=0, Flags=........	22926

Fig-14: Evil Twin attack details

Deauthentication frames in the captured packets are also an evidence for evil twin attack. Figure 13 shows deauthentication frames in the dump file. Figure 14 shows details of evil twin attack. In the alert message when clicking on OK Button details such as source and count of deauthentication frames will display on a new window.

6. CONCLUSIONS

The free Wi-Fi or open Wi-Fi in the open spots is not all safe to use particularly when transferring sensitive data. This paper proposed a forensic analysis framework for open Wi-Fi Network .The forensics process involves capturing network traffic and analyzing captured packets in order to discover the source and destination of packets, URLs visited by the user, detecting DoS attack and evil twin attack. As a future work we can extend the system to collect evidences of all kinds of Dos attacks apart from SYN flood attack and also collect more artefacts of other common attacks in Open Wi-Fi.

REFERENCES

[1] A. H. Lashkari, F. Towhidi and R. S. Hosseini, "Wired Equivalent Privacy (WEP)," 2009 International Conference on Future Computer and Communication, Kuala Lumpar, 2009, pp. 492-495.

[2] A. H. Adnan et al., "A comparative study of WLAN security protocols: WPA, WPA2," 2015 International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, 2015, pp. 165-169.

[3] R. S. Singh, A. Prasad, R. M. Moven and H. K. Deva Sarma, "Denial of service attack in wireless data network: A survey," 2017 Devices for Integrated Circuit (DevIC), Kalyani, 2017, pp. 354-359.

[4] Nadia Benchikha, Mohamed Krim, Khaled Zeraoulia,Chafika Benzaid, ”IWNetFAF: An 57 Integrated Wireless Network Forensic Analysis Framework”, 2016 Cybersecurity and Cyberforensics Conference, pp:35-40, 2016.

[5] Niharika Sharma, Amit Mahajan, Vibhakar Mansotra, ”Identification and analysis of DoS attack Using Data Analysis tools”, International Journal of Innovative Research in Computer and Communication Engineering, pp:11368-11375, June 2016.

[6] Vishwa Modi, Chandresh Parekh, ”Detection of Rogue Access Point to Prevent Evil Twin Attack in Wireless Network”, International Journal of Engineering Research Technology (IJERT), pp:23-26, April-2017