Client-side Evil-Twin access point detection using beacon-frame delay and wireless network parameter deviation

MSc Research Project
Cyber Security

Abhinav Wakhloo
Student ID: x21156956

School of Computing
National College of Ireland

Supervisor: Arghir Niclolae Moldovan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	…Abhinav Wakhloo…. …………………………………………………………………		
Student ID:	…x21156956………………………………………………………………………… …………………………..		
Programme:	…MSc in Cybersecurity…………..	**Year:**	…2022-23…..
Module:	…MSc Research Project…………………………………………………….........		
Supervisor:	…Arghir Nicolae Moldovan………………………………………………..........		
Submission Due Date:	…..1/2/2023…………………………………………………………………………… ……………………….........		
Project Title:	…Client-side Evil-Twin access point detection using beacon-frame delay and wireless network parameter deviation ………..		
Word Count:	…8826…………….. **Page Count**…………..22…………………………..........		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……………………………………………………………………………………………
……Abhinav Wakhloo…

Date: ……1/2/2023……………………………………………………………………………
……………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□

Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Client-side Evil-Twin access point detection using beacon-frame delay and wireless network parameter deviation

Abhinav Wakhloo
x21156956

Abstract

The use of public Wi-Fi hotspots is beneficial for both users and service providers, with users able to access free wireless internet and service providers gaining potential customers. While users can easily take advantage of accessible Wi-Fi Internet hotspot networks in public, they are more vulnerable to man-in-the-middle (MIMT) attacks such as the Evil-Twin attack. An attacker can eavesdrop on communication channels by setting up an Evil-Twin access point and intercepting sensitive user information such as credentials or credit card numbers. Free open (unencrypted) public Wi-Fi hotspots lack security measures because their main goals are to be easily accessible and to draw customers. Simultaneously, the lack of awareness of the potential risk of connecting to such a network increase the severity of the threat. There is a critical need for client-side tools to assist wireless users in identifying and defending themselves against Evil-Twin attacks at public Wi-Fi hotspots. The focus of this research is to explore this problem and build a detection tool that bridges the gap between the limitations of the existing client-side detection solutions and the need to increase the wireless security of Wi-Fi Hotspots. The development of a prototype client-side Evil-Twin access point detection tool was guided by studying the core concepts, techniques, and specifications. The primary goal of this research thesis was to build a more effective solution by comparing the Wi-Fi auditing tools and wireless adapters available to perform Evil-Twin attacks. The evaluation results of the analysis showed that the detection tool can effectively determine the presence of an Evil-Twin access point.

1 Introduction

The use of the IEEE 802.11 wireless network, or Wi-Fi, has become increasingly popular in recent times. Wi-Fi is a form of wireless local area network (WLAN) technology that allows users to connect to the internet without the need for physical cables. According to a report by Cisco, the number of public Wi-Fi hotspots is projected to reach 628 million by 2023, up from 169 million in 2018.(*Wi-Fi® predictions from Cisco's Annual Internet Report | Wi-Fi Alliance*, 2020). Wi-Fi is becoming the preferred method of connecting to the internet in homes, businesses, and public places, such as libraries and coffee shops. A survey of 15,532 individuals in 15 different countries done by Symantec showed that nearly half of the participants would not wait longer than a few minutes to connect to the Wi-Fi at places such as airports, restaurants, shops, and hotels. ('2017-norton-wifi-risk-report-global-results-summary-en.pdf', no date). While the convenience of free Wi-Fi is attractive to many users, there is a corresponding increase in risk. However, this convenience comes with an increased security risk as these hotspots are often unsecured and vulnerable to malicious attacks.

According to a research paper by (Lotfy *et al.*, 2021), "public free Wi-Fi hotspots are more prone to security risks such as man-in-the-middle attacks, eavesdropping, and data leakage." These attacks can be used to gain access to user data and sensitive information, such as credentials and credit card details, as users connect to these open networks. An Evil-Twin attack is one such man-in-the-middle (MIMT) attack, where the attacker is positioned between the user and the legitimate access point, allowing them to intercept and manipulate traffic passing between the two. Public Wi-Fi hotspots are vulnerable to evil twin attacks because they are generally unprotected and unmonitored. An evil twin attack occurs when an attacker creates a malicious Wi-Fi hotspot with the same name as a legitimate one. This malicious hotspot is designed to capture data and credentials that users enter when they connect to the network. The attacker then uses this data to gain access to the user's account or to infect the user's device with malware. This type of attack is especially dangerous in public places, such as airports or coffee shops, where people are more likely to connect to open Wi-Fi networks without verifying their authenticity.

Detecting an Evil-Twin access point can be difficult as the Evil-Twin access point may be designed to look and behave like a legitimate access point. It is crucial to detect these Evil-Twin access points to protect users and networks from malicious actors. One way to detect an Evil-Twin access point is to look for inconsistencies in the wireless network. For example, if a legitimate wireless network has a specific Service Set Identifier (SSID), then any access points with the same SSID should be treated with suspicion. Similarly, if a legitimate access point is broadcasting on a specific channel, other access points on the same channel should be flagged as suspicious. If a wireless access point is discovered having the same SSID then most devices will try to establish a connection with the SSID having the strongest Received Signal Strength Indicator (RSSI).

(Anmulwar *et al.*, 2014) discuss two main techniques for the recognition of Evil-Twin access points: client-side and server-side. Each of these has its own advantages and disadvantages. The server-side method is less of a burden on the client since any changes and alterations are done on the router, gateway, or switch. However, this approach has a major downside as the client is unable to confirm the validity of the access point. On the other hand, the client-side approach involves the client in the detection process. The downside to this is that any software and driver installation needed must be done on the client.

The goal is to address the problem through the red vs. blue team technique. This approach will enable us to recognize any shared flaws and traits of the tools employed by the attacker and locate means to use them to create a client-side detection tool that can detect the Evil-Twin access point. In this thesis, the primary focus is comparing the tools Airgeddon, Fluxion, and Pineapple Tetra used by attackers to create Evil-Twin access points. And also by examining the various wireless adapters like TL-WN8223N, AWSU036ACH, and Hak5 Wi-Fi Pineapple Tetra to determine which one is the most compatible with the tools used to conduct these attacks. The working combinations help build the different experiment setups for the research. The detection strategy can then be refined by assessing the outcomes of multiple experiments. A client-side detection technique was chosen to tackle the Evil-Twin access point issue. Compared to previous research, this approach has several benefits. Our detection technique does not create a filter list or require the signature of the legitimate access points prior to detection. At the same time, our approach does not require an additional server to be deployed. Furthermore, a more comprehensive assessment reveals that the tools often imitate other parameters, such as the Service Set Identifier, Channel Number, and Media Access Control address. It was observed that the tools Airgeddon and Fluxion do not alter the Vendor Specific information while creating the Evil-Twin. At the same time, Pineapple Tetra strips the Vendor Specific information from the packets. This parameter helps in identifying the presence of another device. Subsequently, the detection parameters chosen in the final analysis, such as RSSI, Timestamp, Sequence number, and Vendor-Specific information, help accurately identify the presence of an Evil-Twin access point.

Additionally, Group Cipher Suite, which provides the encryption method used, and Auth Key Management Suite, which shows the authentication method used, were observed to be absent while creating the Evil-Twin access point. Similarly, the RSSI value recorded over the various setups shows that the legitimate access points have consistent values compared to the Evil-Twin access point. Also, the Timestamp delay between the consecutive Beacon frames of the legitimate access point was consistent as opposed to the Evil-Twin access point. Thus, the following parameters contribute to the uniqueness while adding novelty to the research and helping to distinguish it from other studies,

- Vendor Specific Information
- Group Cipher Suite
- Auth Key Management Suite

Therefore, the Vendor Specific Information, Group Cipher Suite, and Auth Key Management Suite are essential parameters for identifying Evil-Twin access points. These parameters, along with timestamps of beacon frames and RSSI, are used to improve the precision of the detection tool.

1.1 Research Question

In order to carry out a detailed and concise scope of research, this thesis is directed by the following research question.

How can we safeguard users against malicious actors by analysing and detecting Evil-Twin access points using beacon-frame delay and wireless network parameter deviation?

Based on this research question, numerous sub-questions emerge that will facilitate a meticulous and comparative analysis. The thesis was guided by these sub-questions that outlined the specific objectives, which in turn formed the basis of the conceptual framework.

These sub-questions are,

What are the various tools to create an Evil-Twin access point?
What are the various wireless adapters required to enable these tools?
Which wireless parameters can be utilized to differentiate between the legitimate and Evil-Twin access points?
Which combination of wireless adapters and tools will create an Evil-Twin that will be harder to detect?

Considering and focusing on these questions and conducting extensive research will assist and guide the research work.

1.2 Research Objective

This dissertation aims to create a system/tool that enables wireless users to identify and protect themselves from malicious evil twin attacks while using free open public Wi-Fi hotspots. The main objective of this research thesis was to create a more effective, efficient, and practical client-side detection tool by comprehensively analysing the various wireless adapters and tools.

1.3 Structure of the Report

The structure report consists of following sections: related work, research methodology, design specification, implementation, evaluation, discussion, conclusion, and references.

In related work section, the comprehensive review of the relevant literature on the detection of Evil-Twin access points is highlighted. It includes an overview of the key concepts, theories, and studies related to the Evil-Twin access points, focusing on recent work and findings. The literature review provides a framework for this research paper and helps to identify potential gaps in the current research. Additionally, the review provides a basis for the research paper, helping to shape the focus and scope of the study. The design specifications section of the report focuses on the various hardware and the tools required to create Evil-Twin access points and helps to narrow down the different parameters required for a comprehensive analysis. The implementation section on the thesis shows how the research methodology was implemented to build the detection tool. In the evaluation shows the observations and the findings from the various experimental setups. The discussions section highlights of the overall findings of the detection tool. Finally, the thesis is concluded, summarizing the research's main points and findings.

2 Related Work

This section of the report provides a comprehensive review of pertinent literature related to wireless security, the need for secure free open public Wi-Fi networks, client-side evil twin attack detection solutions, and research methodology. The literature review aims to identify existing studies, their strengths and weaknesses, and any gaps in the literature. The goal of the literature review is to guide the development of a system for users to independently detect and protect themselves from Evil-Twin access point attacks while using free open public Wi-Fi hotspots.

The research proposed by the authors (Kao *et al.*, 2014) discuss the use of the timestamps of the sequential Beacon Frames received and analysed the difference in the timestamps received of two consecutive sequential frames and found that there notable distinction between the timestamps of legitimate and Evil-Twin access points. Even if the attacker synchronises the sequence of the Beacon frames and the received timestamp the distinction remains. Although there is a way to detect the presence of the Evil-Twin with this approach, but it is impossible to identify without prior evaluation of the legitimate access point. (Ketkhaw and Thipchaksurar, 2017) authors have implemented the detection of the Rogue access points by using the SSID parameter and comparing them with the Probe and Beacon requests.

The authors (Amoordon *et al.*, 2022) have employed the Beacon frame interval and Sequence number gap in the detection of Evil-Twin and detecting Jamming attacks. This approach can be improved by adding more parameters. (Alotaibi and Elleithy, 2015) has used the size of Beacon Frame (BFS) packets and matches it against threshold value (TSV). This method of detection gathers the BFS of all the frames and then compares the values to the set TSV value to detect the presence of the Evil-Twin attack. (Vanjale and Mane, 2014) authors approach in detection is based on collecting the collecting the SSID and corresponding MAC and RSSI values and then comparing the deviation of the RSSI values to identify the Evil-Twin access point. (Mwinuka *et al.*, 2022) authors have implemented their detection methodology for detecting Evil-Twin access points on Android Devices by focusing on the RSSI deviation and achieved a high rate of accuracy. However, more parameters can be added to provide to achieve a higher accuracy as the signal strength can be increased by the attacker.

(Kitisriworapan, Jansang and Phonphoem, 2019) have discussed the detection of Evil-Twin access points using the Modulation Coding Scheme (MCS) and Round-Trip-Time (RTT) parameters in detection. This method shows a higher rate of detection when both the parameters are used together. However, more parameters are required as to increase the accuracy.

(Yang, Song and Gu, 2012) have proposed the use of statistical approach in detecting the Evil-Twin access points by employing two algorithms. However, the algorithms are based on the traffic load performance by evaluating the Transmission Control Protocol (TCP) and Internet Control Message protocol (ICMP) parameters of the legitimate access point and in heavy loads the accuracy of the detection algorithm decreases. The authors (Zhang *et al.*, 2020) have proposed to use the ICMP travel between wireless network clients through their gateway and the dedicated internet server. The drawback of the method is the sample size of the data that was collected. For higher accuracy of detection a significantly large data sample must be collected. (Burns *et al.*, 2017) authors approach uses traceroute in the detection and comparing the Time-To-Live (TTL) parameter deviation to distinguish between the access points. The drawback of this solution relies on an external server.

(Asaduzzaman, Majib and Rahman, 2020) authors have employed a machine learning approach for detection using a feature set of various parameters. However, this approach is not suitable for performing check on live traffic and accuracy is impacted if the attacker sending malformed packets. (Nakhila and Zou, 2016) have discussed the provides extremely high rate of detection using Info packets but relies on dedicated server to be deployed to assist in the detection. (Lovinger *et al.*, 2020) the authors have used various parameters such as the SSID, Basic Service Set Identifier (BSSID), channel, Security, Country, and Basic Bit Rates to perform the detection. However, the approach requires the need of capturing a signature which is used to differentiate between the legitimate and Evil-Twin access point.

(Lanze *et al.*, 2015) authors have used Timing Synchronization Function (TSF) timestamps to help identify and distinguish between the access points. (Jadhav, Vanjale and Mane, 2014) have used the clock Skew method to perform the detection of the Evil-Twin access. The TSF time stamps are used to calculate the Clock Skew on access point. The drawback of this technique is that requires the fingerprint of the legitimate access point for comparison.

The research proposed by the authors (Jang *et al.*, 2020) using intentional Channel interference across the various channel of 802.11 range. With their method they were able to get hight rate of accuracy.

3 Research Methodology

In this section of the thesis, the research methodology employed is detailed and a comprehensive comparative analysis is defined and discussed in detecting Evil-Twin access created using various tools and wireless adapters. The following steps have been considered to develop the methodology to detect the Evil-Twin access points.

- Select the different wireless auditing and social engineering tools that will assist in creating the Evil-Twin access point.
- Identify the various wireless adapters that are compatible with the tools.
- Creating Evil-Twin access points with various combinations of tools and wireless adapters.
- Capturing the network traffic to understand the various parameters that will assist in detecting the presence of Evil-Twin access points.
- Identifying the tools and dependencies required to create the detection tool.
- Selecting the parameters and identifying the Evil-Twin using the detection tool.

According to previous research, Evil-Twin access point detection techniques can be divided into active or client-side detection and passive or server-side detection (Anmulwar *et al.*, 2014). Both methods have their own strengths and weaknesses, when it comes to detecting an Evil-Twin. Several papers make use of the client-side approach, which utilizes the round trip time out (RTT) network metric to detect both the client machine and local server, as seen in (Kitisriworapan, Jansang and Phonphoem, 2019). According to (Mwinuka *et al.*, 2022), the use of the RSSI metric provides a 98% and 99% accuracy rate when applied to open and closed networks, respectively. It is possible to distinguish Evil-Twin access points from legitimate ones by looking at various parameters, such as SSID, BSSID, RSSI and encryption. Comparing these elements can help to differentiate between the two.

The authors (Kao *et al.*, 2014) proposed research about the use of timestamps found in sequential Beacon Frames. They discovered that there was a large difference between the timestamps of legitimate and Evil-Twin access points. Even if the attacker attempted to synchronize the timestamps, the distinction still remained. While a way to detect the presence of the Evil-Twin has been unveiled, it is not possible to identify it without prior knowledge of the legitimate access point. In a later study, (Ketkhaw and Thipchaksurar, 2017) developed a method to detect Rogue access points by comparing SSID parameters of Probe and Beacon requests. Based on the results of the research work performed, the parameters necessary for identifying and evaluating the Evil-Twin access points can be regulated. The client-side passive technique requires us to consider the Received Signal Strength Indicator, Destination MAC, Source MAC, AP MAC, Frequency Channel, Beacon Interval, Timestamp, Sequence Number, Cipher, Suite, Service Set Identifier, Vendor, and Chipset information.

4 Design Specification

This section of the thesis will review the hardware and software used to use our research methodology and create a conducive environment to help develop the detection tool.

4.1 Hardware

The setup first requires a Debian-based Linux distribution running as a virtual machine on top of the base host machine. The virtualization software used is Parallels Desktop 17. The specifications of the host machine are listed below in Table 1, and the specifications of the Virtual machine used are listed in Table 2. Furthermore, various wireless adapters are used to build the various test cases for the experiment.

Table 1: Shows the specification of the Host machine

Host Machine	M1 MacBook Pro
Processor	8-core CPU with 4 performance cores and 4 efficiency cores
System Architecture	ARM-64
Operating System	Ventura 13.0.1
RAM	8 GB

Table 2: Shows the specifications of the Virtual Machine

Virtual Machine	Kali Linux
Processor	2-core CPU
System Architecture	ARM-64
Operating System	Kali 2022.4
RAM	2 GB

To create Evil-Twin access points various wireless adapters were used. The following Table 3 shows the specifications of the adapters. These adapters were selected as per the compatibility with the wireless auditing and social engineering tools.

Table 3: Shows the specifications of the wireless adapters

Device	TP-Link	Alfa Network	Hak5 Wi-Fi Pineapple
Model	TL-WN8223N	AWSU036ACH	Pineapple Tetra
Band	2.4GHz	2.4GHz and 5GHz	2.4GHz and 5GHz

Chipset	Realtek RTL8192EU	Realtek RTL8812AU	Atheros AR9344 and AR9580
IEEE 802.11 Standards	b/g/n	a/b/g/n/ac	a/b/g/n
Antenna	Single (Internal)	2	4
Transmit Power	<20dbm	2 dipole omi (5 dBi gain)	29dBm gain

The default drivers for the TP-Link adapter do not have all the required modes available to create the Evil-Twin attack. The Default modes are managed and monitor. Whereas the modes AP is also required to successfully create the Evil-Twin access point. Similarly, for the Alfa Network adapter the default drivers are not compatible with Kali Linux and the adapter remains undetected. For both adapters it is required to update the adapters to their compatible drivers. These adapters are used to create the used in the case study 1 and case study 2 for the tool Airgeddon and Fluxion.

The Legitimate access point used in the setup is created by using the Android Device OnePlus 8 pro. At the same time, the client devices used in all the case studies are two phones, iPhone XR and Xiaomi K20 Pro, and a windows laptop Lenovo ThinkPad E15 Gen2. Table 4 highlights the specifications of the client devices used in this research.

Table 4: Shows the device specification of the devices

Device Type	Phone	Phone	Phone	Laptop
Model	iPhone XR	OnePlus 8 Pro	K20 Pro	ThinkPad E15 Gen2
Manufacturer	Apple	OnePlus	Xiaomi	Lenovo
Operating System	iOS version 16.1.2	Android 13.0	Android 10	Windows 11(Version 21H2)
Chipset	Broadcom	Qualcomm	Qualcomm	Intel

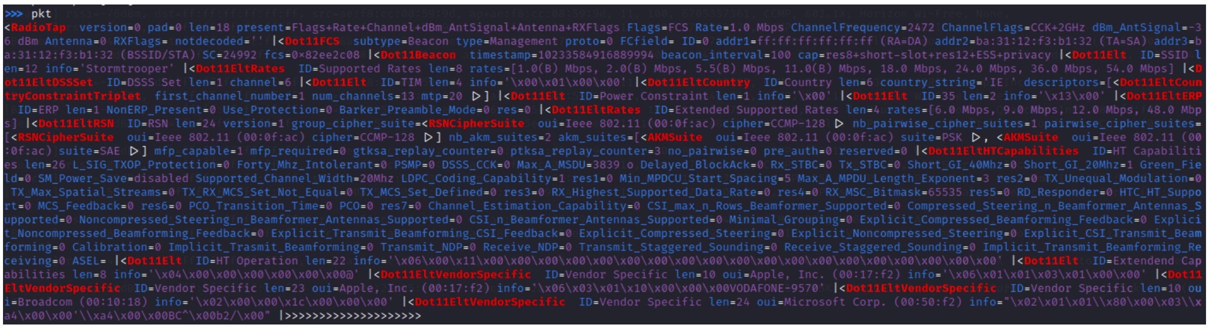
4.2 Software Tools

Various software tools are used for this research thesis. These tools include wireless auditing and social engineering tools such as Airgeddon and Fluxion. The tool Scapy is used to capture the Beacon frames generated by the legitimate access point and the Evil-Twin access point in all the three case studies.

Airgeddon is an open-source Linux-based wireless network security auditing tool. It is designed to perform a wide range of wireless security auditing tasks, including scanning for wireless networks, cracking WEP and WPA-PSK keys, generating WPS pin codes, and many more. It also includes a collection of additional tools and features, such as a MAC address changer and Evil-Twin access point creator. Along with the Evil-Twin access point creation, the tool can also deploy a captive portal to perform social engineering attacks. The WPA handshake capture by the tool is used to verify the password captured from the captive portal.

Fluxion is a wireless security auditing and social-engineering tool. It is used to audit Wi-Fi networks and is capable of attacking WPA and WPA2 networks. It is a tool intended to be used for legal security purposes only. Fluxion can be used to test the security of a Wi-Fi network by using social engineering techniques. It can be used to break WPA and WPA2 passwords by generating a fake access point and then capturing the handshake of a user who has connected to the fake access point. It can also be used to carry out a man-in-the-middle attack to capture user credentials or other sensitive information. Fluxion is a powerful tool that can be used to audit the security of a wireless network.

Scapy is a powerful packet manipulation program and library written in Python. It is used to craft, inject, analyse, and decode network packets, as well as to create and manipulate Wi-Fi frames. Scapy can be used to execute a wide variety of tasks, such as scanning, tracerouting, probing, unit tests, attack, and network discovery. Scapy can also be used to craft and send custom packets for troubleshooting purposes and for network audits. Scapy has a powerful set of capabilities, including the ability to sniff, forge, and decode packets, as well as send and receive custom packets. It can also be used to perform an active scan, trace a path, and probe for open ports. Scapy also supports sniffing on multiple interfaces at the same time, as well as the ability to filter captured packets, as seen in Figure 1. Scapy also provides a powerful scripting language that can be used to automate tasks such as scanning and packet manipulation. Scapy is also extensible and can be extended to include custom protocol dissectors and packet crafting modules. Scapy is a powerful and resourceful tool for network professionals, and it can be used to perform a wide variety of tasks, such as troubleshooting, security assessment, and network analysis.



```
>>> pkt
<RadioTap  version=0 pad=0 len=18 present=Flags+Rate+Channel+dBm_AntSignal+Antenna+RXFlags Flags=FCS Rate=1.0 Mbps ChannelFrequency=2472 ChannelFlags=CCK+2GHz dBm_AntSignal=-3
6 dBm Antenna=0 RXFlags= notdecoded='' |<Dot11FCS  subtype=Beacon type=Management proto=0 FCfield= ID=0 addr1=ff:ff:ff:ff:ff:ff (RA=DA) addr2=ba:31:12:f3:b1:32 (TA=SA) addr3=b
a:31:12:f3:b1:32 (BSSID/STA) SC=24992 fcs=0×82ee2c08 |<Dot11Beacon  timestamp=10233584916889994 beacon_interval=100 cap=res8+short-slot+res12+ESS+privacy |<Dot11Elt  ID=SSID l
en=12 info='Stormtrooper' |<Dot11EltRates  ID=Supported Rates len=8 rates=[1.0(B) Mbps, 2.0(B) Mbps, 5.5(B) Mbps, 11.0(B) Mbps, 18.0 Mbps, 24.0 Mbps, 36.0 Mbps, 54.0 Mbps] |<D
ot11EltDSSSet  ID=DSSS Set len=1 channel=6 |<Dot11Elt  ID=TIM len=4 info='\x00\x01\x00\x00' |<Dot11EltCountry  ID=Country len=6 country_string='IE ' descriptors=[<Dot11EltCoun
tryConstraintTriplet  first_channel_number=1 num_channels=13 mtp=20 ▷] |<Dot11Elt  ID=Power Constraint len=1 info='\x00' |<Dot11Elt  ID=35 len=2 info='\x13\x00' |<Dot11EltERP
  ID=ERP len=1 NonERP_Present=0 Use_Protection=0 Barker_Preamble_Mode=0 res=0 |<Dot11EltRates  ID=Extended Supported Rates len=4 rates=[6.0 Mbps, 9.0 Mbps, 12.0 Mbps, 48.0 Mbp
s] |<Dot11EltRSN  ID=RSN len=24 version=1 group_cipher_suite=<RSNCipherSuite  oui=Ieee 802.11 (00:0f:ac) cipher=CCMP-128 ▷ nb_pairwise_cipher_suites=1 pairwise_cipher_suites=
[<RSNCipherSuite  oui=Ieee 802.11 (00:0f:ac) cipher=CCMP-128 ▷] nb_akm_suites=2 akm_suites=[<AKMSuite  oui=Ieee 802.11 (00:0f:ac) suite=PSK ▷, <AKMSuite  oui=Ieee 802.11 (00
:0f:ac) suite=SAE ▷] mfp_capable=1 mfp_required=0 gtksa_replay_counter=0 ptksa_replay_counter=3 no_pairwise=0 pre_auth=0 reserved=0 |<Dot11EltHTCapabilities  ID=HT Capabiliti
es len=26 L_SIG_TXOP_Protection=0 Forty_Mhz_Intolerant=0 PSMP=0 DSSS_CCK=0 Max_A_MSDU=3839 o Delayed_BlockAck=0 Rx_STBC=0 Tx_STBC=0 Short_GI_40Mhz=0 Short_GI_20Mhz=1 Green_Fie
ld=0 SM_Power_Save=disabled Supported_Channel_Width=20Mhz LDPC_Coding_Capability=1 res1=0 Min_MPDCU_Start_Spacing=5 Max_A_MPDU_Length_Exponent=3 res2=0 TX_Unequal_Modulation=0
 TX_Max_Spatial_Streams=0 TX_RX_MCS_Set_Not_Equal=0 TX_MCS_Set_Defined=0 res3=0 RX_Highest_Supported_Data_Rate=0 res4=0 RX_MSC_Bitmask=65535 res5=0 RD_Responder=0 HTC_HT_Suppo
rt=0 MCS_Feedback=0 res6=0 PCO_Transition_Time=0 PCO=0 res7=0 Channel_Estimation_Capability=0 CSI_max_n_Rows_Beamformer_Supported=0 Compressed_Steering_n_Beamformer_Antennas_S
upported=0 Noncompressed_Steering_n_Beamformer_Antennas_Supported=0 CSI_n_Beamformer_Antennas_Supported=0 Minimal_Grouping=0 Explicit_Compressed_Beamforming_Feedback=0 Explici
t_Noncompressed_Beamforming_Feedback=0 Explicit_Transmit_Beamforming_CSI_Feedback=0 Explicit_Compressed_Steering=0 Explicit_Noncompressed_Steering=0 Explicit_CSI_Transmit_Beam
forming=0 Calibration=0 Implicit_Trasmit_Beamforming=0 Transmit_NDP=0 Receive_NDP=0 Transmit_Staggered_Sounding=0 Receive_Staggered_Sounding=0 Implicit_Transmit_Beamforming_Re
ceiving=0 ASEL= |<Dot11Elt  ID=HT Operation len=22 info='\x06\x00\x11\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00' |<Dot11Elt  ID=Extendend Cap
abilities len=8 info='\x04\x00\x00\x00\x00\x00\x00@' |<Dot11EltVendorSpecific  ID=Vendor Specific len=10 oui=Apple, Inc. (00:17:f2) info='\x06\x01\x01\x03\x01\x00\x00' |<Dot11
EltVendorSpecific  ID=Vendor Specific len=23 oui=Apple, Inc. (00:17:f2) info='\x06\x03\x01\x10\x00\x00\x00VODAFONE-9570' |<Dot11EltVendorSpecific  ID=Vendor Specific len=10 ou
i=Broadcom (00:10:18) info='\x02\x00\x00\x1c\x00\x00\x00' |<Dot11EltVendorSpecific  ID=Vendor Specific len=24 oui=Microsoft Corp. (00:50:f2) info="\x02\x01\x01\\x80\x00\x03\\x
a4\x00\x00'\\xa4\x00\x00BC^\x00b2/\x00" |>>>>>>>>>>>>>>>>>>>>
```

Figure 1: Shows the beacon Frame captured by using Scapy

4.3 Detection Script

The **detection tool** is built using Python and Scapy, which performs live capture of the Beacon frames transmitted by the wireless adapters in the experiment. The detection tool uses the sniff function provided by Scapy to collect beacon frames. Scapy also helps extract parameters such as RSSI, Destination MAC, Source MAC, AP MAC, Channel, Beacon Interval, Timestamp, Sequence number, Cipher, Suite, SSID, Vendor, and Chipset, as highlighted in the research methodology. The output of the data gathered by the tool is extracted in a **.**CSV file using the Pandas Library. The Vendor information is extracted and updated in the output file using Python Libraries such as mac-vendor-lookup 0.1.12 and macaddress 2.0.2.

5 Implementation

To implement our proposed research methodology, the implementation has been divided by setting up three test case studies.

In **case study 1**, the tool Airgeddon was used to create the Evil-Twin access point. First, the TP-Link TL-WN8223N adapter was used with the default driver. The tool Airgeddon performs the Evil-Twin attack in mainly two stages, capture the WPA handshake and create the Evil-Twin with a captive portal. The wireless adapter is set to monitor mode to prepare the adapter for the attack. The successful completion of the steps is recorded. Then the scenario is repeated by updating the driver of the TP-Link TL-WN8223N adapter. After successfully creating the Evil-Twin access point, the detection tool is engaged to capture the beacon frames. The Detection tool requires a wireless adapter to capture the data. The captured .CSV file is then analysed. Similarly, the scenario is repeated for the Alfa Network (AWSU036ACH) adapter.

In **case study 2**, Fluxion tool was used to create the Evil-Twin access point. First, the TP-Link TL-WN8223N adapter was used with the default driver. The tool Fluxion performs the Evil-Twin attack in mainly two stages, capture the WPA handshake and create the Evil-Twin with a captive portal. The wireless adapter is set to monitor mode to prepare the adapter for the attack. The successful completion of the steps is recorded. The scenario is repeated after updating the driver of the TP-Link TL-WN8223N adapter. After successfully creating the Evil-Twin access point, the detection tool is utilized to capture the beacon frames. The Detection tool requires a wireless adapter to capture the data. The capture .CSV file is then analysed. Similarly, the scenario is repeated for the Alfa Network (AWSU036ACH) adapter.

Additionally, it was observed that the Fluxion tool requires two adapters to be used together, where one is used as a Tracking and Jamming interface, and the other is used for the creation of AP. Here, the experiment was performed using the TP-Link TL-WN8223N adapter as the Tracking and Jamming interface and Alfa Network (AWSU036ACH) adapter as the AP interface. In the second scenario, Alfa Network (AWSU036ACH) adapter was used as the Tracking and Jamming interface, and the TP-Link TL-WN8223N adapter was used as the AP interface. After successfully creating the Evil-Twin access point, the detection tool was utilized to capture the beacon frames. The Detection tool requires a wireless adapter to capture the data. The capture .CSV file is then analysed.

In **case study 3**, Hak5 pineapple Tetra was used to create an Evil-Twin access point. Hak5 pineapple Tetra uses its PineAP Suite to perform the Evil-Twin attack. In order to create the captive portal using the Hak5 pineapple Tetra, the EvilPortal module must be installed. The Hak5 Pineapple Tetra is then able to capture the credentials of the user using the captive portal. After the successful creation of the Evil-Twin access point, the detection tool is utilized to capture the beacon frames. The Detection tool requires a wireless adapter to capture the data. The captured .CSV file is then analysed.

The setup for the experiments is highlighted in the Figure 2 below.

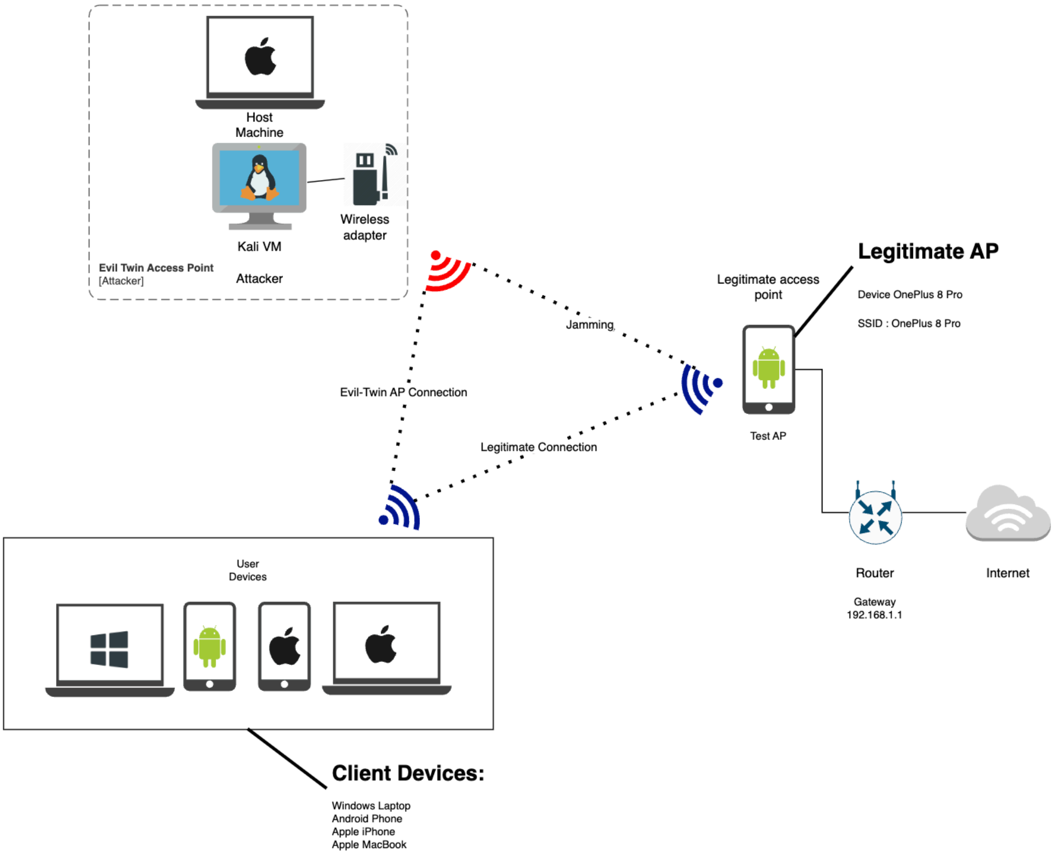


Figure 2: The setup for the experiment

Detection Tool:

The detection tool is developed following the research methodology using Python. The Scapy Library is used to capture the packets generated by the wireless adapters. The output of the data gathered by the tool is extracted in a .CSV file by using the Pandas Library. The Vendor information is extracted and updated in the output file using the Python Libraries such as mac-vendor-lookup 0.1.12 and macaddress 2.0.2. The working of the detection tool can be understood by observing the flow chart of the tool as shown in Figure 3. Furthermore, the tool airmon-ng is required to setup the interface in monitor mode to capture the packets.

The detection procedure is as follows,
Step 1: Prepare the wireless adapter to be used by the script by putting the interface in monitor mode.
Step 2: The system processes networking and NetworkManager must be stopped prior to running the tool by using the airmon-ng tool.

Step 3: The interface name must be passed along with the count interval at time of running the tool.
Step 4: The tool will capture the packets using the sniff function provided by the Scapy library.
Step 5: Only the beacon frames are considered by the tool.
Step 6: The RSSI, Destination MAC, Source MAC, AP MAC, Channel, Beacon Interval, Timestamp, Sequence number, Cipher, Suite, SSID, Vendor, and Chipset are captured.
Step 7: The extracted information is saved in the form of a .CSV file as seen in the Figure 4.

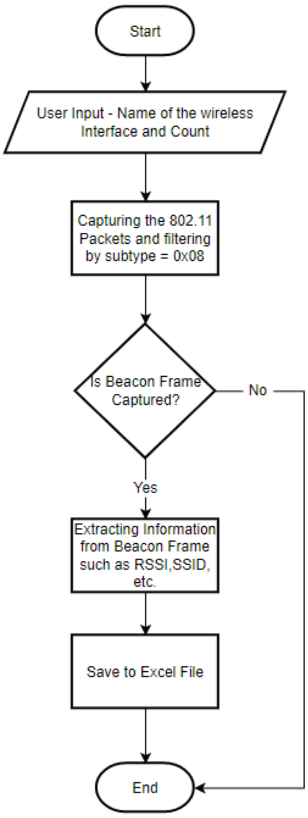
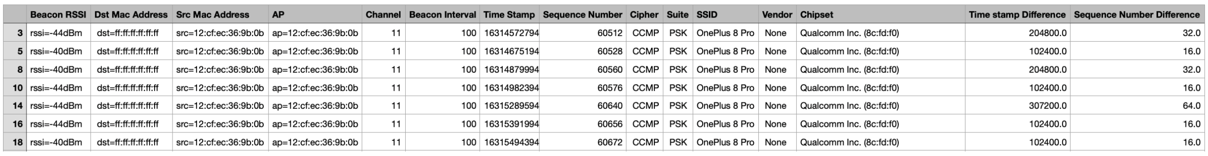

Start
User Input - Name of the wireless Interface and Count
Capturing the 802.11 Packets and filtering by subtype = 0x08
Is Beacon Frame Captured?
No
Yes
Extracting Information from Beacon Frame such as RSSI,SSID, etc.
Save to Excel File
End

Figure 3: Flow chart of the proposed detection tool



	Beacon RSSI	Dst Mac Address	Src Mac Address	AP	Channel	Beacon Interval	Time Stamp	Sequence Number	Cipher	Suite	SSID	Vendor	Chipset	Time stamp Difference	Sequence Number Difference
3	rssi=-44dBm	dst=ff:ff:ff:ff:ff:ff	src=12:cf:ec:36:9b:0b	ap=12:cf:ec:36:9b:0b	11	100	16314572794	60512	CCMP	PSK	OnePlus 8 Pro	None	Qualcomm Inc. (8c:fd:f0)	204800.0	32.0
5	rssi=-40dBm	dst=ff:ff:ff:ff:ff:ff	src=12:cf:ec:36:9b:0b	ap=12:cf:ec:36:9b:0b	11	100	16314675194	60528	CCMP	PSK	OnePlus 8 Pro	None	Qualcomm Inc. (8c:fd:f0)	102400.0	16.0
8	rssi=-40dBm	dst=ff:ff:ff:ff:ff:ff	src=12:cf:ec:36:9b:0b	ap=12:cf:ec:36:9b:0b	11	100	16314879994	60560	CCMP	PSK	OnePlus 8 Pro	None	Qualcomm Inc. (8c:fd:f0)	204800.0	32.0
10	rssi=-44dBm	dst=ff:ff:ff:ff:ff:ff	src=12:cf:ec:36:9b:0b	ap=12:cf:ec:36:9b:0b	11	100	16314982394	60576	CCMP	PSK	OnePlus 8 Pro	None	Qualcomm Inc. (8c:fd:f0)	102400.0	16.0
14	rssi=-44dBm	dst=ff:ff:ff:ff:ff:ff	src=12:cf:ec:36:9b:0b	ap=12:cf:ec:36:9b:0b	11	100	16315289594	60640	CCMP	PSK	OnePlus 8 Pro	None	Qualcomm Inc. (8c:fd:f0)	307200.0	64.0
16	rssi=-44dBm	dst=ff:ff:ff:ff:ff:ff	src=12:cf:ec:36:9b:0b	ap=12:cf:ec:36:9b:0b	11	100	16315391994	60656	CCMP	PSK	OnePlus 8 Pro	None	Qualcomm Inc. (8c:fd:f0)	102400.0	16.0
18	rssi=-40dBm	dst=ff:ff:ff:ff:ff:ff	src=12:cf:ec:36:9b:0b	ap=12:cf:ec:36:9b:0b	11	100	16315494394	60672	CCMP	PSK	OnePlus 8 Pro	None	Qualcomm Inc. (8c:fd:f0)	102400.0	16.0

Figure 4: Snippet of the data extracted by the tool

6 Evaluation

This section of the master thesis demonstrates and analyses the effectiveness of the proposed methodology by comparing the detection of various Evil-Twin access points created by employing different wireless adapters and tools. The efficacy of the detection tool developed is evaluated. In this research, two Wi-Fi security auditing and social engineering tools, Airgeddon and fluxion, were used to create the Evil-Twin access points with the combination of three wireless adapters, TP-Link (TL-WN8223N), Alfa Network (AWSU036ACH) and

Hak5 Wi-Fi Pineapple Tetra, and their results were recorded and analysed separately. After creating the Evil-Twin access points, three devices were used as client machines, and their corresponding results were recorded. The Detection tool captured the Beacon Frame packets from the access points. Selected parameters extract the relevant data and is stored in the form of an excel sheet, which help visualize the differences between the legitimate and Evil-Twin access points. With this data, graphs are created that help perform a comparative analysis and highlight the key differences to identify the Evil-Twin access points.

6.1 Case Study 1: Airgeddon

In this setup, the tool Airgeddon was used to create the Evil-Twin access point using two wireless adapters, TP-Link (TL-WN8223N) and Alfa Network (AWSU036ACH). The steps of creating an Evil-Twin access point were identified and summarized. The ability of the wireless adapters to execute the steps was recorded in the table. These were tested against three client devices and the observations are recorded separately.

TP-Link (TL-WN8223N):

The TP-Link (TL-WN8223N) adapter was first used with its default driver RTL8xxxu to build an Evil Twin access point. It was noted in the findings that the adapter with its default driver could only execute the first phase of the attack, which is capturing the WPA handshake, and was unable to create an Evil-Twin access point. After updating the driver of the card with version 4.4.x, the adapter was able to create the Evil-Twin access point.

Alfa Network (AWSU036ACH):

The Alfa Network (AWSU036ACH) adapter is a dual-band wireless adapter and is not detected in Kali Linux when running on the default driver RTL88xxau. After updating the driver of the adapter to version 5.6.2 it is possible to perform a complete Evil-Twin attack. While using the Alfa Network card both 2.4GHz and 5GHz bands can be used, which enables to perform attack on wireless network on the both the wireless bands.

Table 5 : Compatibility of the wireless adapters with Airgeddon Tool

Device	TP-Link	TP-Link	Alfa Network	Alfa Network	Alfa Network	Alfa Network
Band	2.4GHz	2.4GHz	2.4GHz	5GHz	2.4GHz	5GHz
Model	TL-WN8223N	TL-WN8223N	AWSU036ACH	AWSU036ACH	AWSU036ACH	AWSU036ACH
Driver	Default (RTL8xxxu)	v4.4.x	Default (RTL88xxau)	Default (RTL88xxau)	v5.6.4.2	v5.6.4.2
Chipset	Realtek RTL8192EU	Realtek RTL8192EU	Realtek RTL8812AU	Realtek RTL8812AU	Realtek RTL8812AU	Realtek RTL8812AU
Modes Supported	Managed, Monitor	IBSS, Managed, AP, Monitor, P2P-Client, P2P-Go	Managed, Monitor	Managed, Monitor	IBSS, Managed, AP, Monitor, P2P-Client, P2P-Go	IBSS, Managed, AP, Monitor, P2P-Client, P2P-Go
Setting interface in monitor mode	✓	✓	✗	✗	✓	✓

Reset Attack on Client	✓	✓	✗	✗	✓	✓
De-authenticating Client	✓	✓	✗	✗	✓	✓
Capturing WPA/WPA2 Handshake	✓	✓	✗	✗	✓	✓
Evil Twin AP creation	✗	✓	✗	✗	✓	✓
Captive portal to steal passwords	✗	✗	✗	✗	✓	✓

Based on the above observations seen in Table 5, it can be concluded that Alfa Network (AWSU036ACH) adapter is the only adapter capable of successfully creating the Evil-Twin access point along with the captive portal. As observed in the Table 6, after connecting the client devices, it was observed that only the Apple iPhone was unable to see the legitimate access point, while the Android Phone and the windows laptop were able to see both the access points in their available networks. It was also noted that all clients were unable to connect to the legitimate access point during the attack.

Table 6: Observations on Client devices for Airgeddon Tool

Client Devices	**Apple iPhone**	**Android Phone**	**Windows Laptop**
User required to reconnect manually to AP after WPA handshake attack.	✗	✗	✗
Device reconnects automatically to AP after WPA handshake attack.	✓	✓	✓
Legitimate AP seen along with Evil-Twin	✗	✓	✓
Able to connect to legitimate AP during rouge AP attack	✗	✗	✗
Captive portal seen.	✓	✓	✓

6.2 Case Study 2: Fluxion

In this setup, the Evil-Twin access points were created using the Fluxion tool. The Fluxion tool requires two wireless adapters to perform a complete Evil-Twin attack, while using only one adapter can only perform the first phase of the attack. The results obtained while using individual adapters is recorded in the below Table 7.

Table 7: Compatibility of wireless adapters with Fluxion Tool

Device	TP-Link	TP-Link	Alfa Network	Alfa Network	Alfa Network	Alfa Network
Band	2.4GHz	2.4GHz	2.4GHz	5GHz	2.4GHz	5GHz
Model	TL-WN8223N	TL-WN8223N	AWSU036ACH	AWSU036ACH	AWSU036ACH	AWSU036ACH
Driver	Default (RTL8xxxu)	v4.4.x	Default (RTL88xxau)	Default (RTL88xxau)	v5.6.4.2	v5.6.4.2
Chipset	Realtek RTL8192EU	Realtek RTL8192EU	Realtek RTL8812AU	Realtek RTL8812AU	Realtek RTL8812AU	Realtek RTL8812AU
Modes Supported	Managed, Monitor	IBSS, Managed, AP, Monitor,	Managed, Monitor	Managed, Monitor	IBSS, Managed, AP, Monitor, P2P-Client, P2P-Go	IBSS, Managed, AP, Monitor, P2P-Client, P2P-Go

		P2P-Client, P2P-Go				
Setting interface in monitor mode	✓	✓	✗	✗	✓	✓
Reset Attack on Client	✓	✓	✗	✗	✓	✓
De-authenticating Client	✓	✓	✗	✗	✓	✓
Capturing WPA/WPA2 Handshake	✓	✓	✗	✗	✓	✓
Evil Twin AP creation	✗	✗	✗	✗	✗	✗
Captive portal to steal passwords	✗	✗	✗	✗	✗	✗

While performing the attack when using two wireless interfaces, one must be selected as the Target Tracker and Jamming interface while the other must be used as the AP interface. In this experiment both adapters were used in combinations to perform the attack and the observations were noted in the below Table 8.

Table 8: Performance of Fluxion Tool when combination of wireless adapter used

Device	TP-Link	Alfa Network	TP-Link	Alfa Network
Model	TL-WN8223N	AWSU036ACH	TL-WN8223N	AWSU036ACH
Attack interface type	Target tracker interface	AP interface	AP interface	Target tracker interface
Setting interface in monitor mode	✓		✓	
Reset Attack on Client	✓		✓	
De-authenticating Client	✓		✓	
Capturing WPA/WPA2 Handshake	✓		✓	
Evil Twin AP creation	✗		✓	
Captive portal to steal passwords	✗		✓	

Based on the above observations seen in Table 8, it can be concluded that Evil-Twin attack is only possible when the Alfa Network (AWSU036ACH) adapter is used as the Target Tracker interface while TP-Link (TL-WN8223N) adapter is used for the AP interface. After the Evil-Twin is created the Client devices are connected and the observations are recorded in a tabular form in the below Table 9.

Table 9: Observations on Client devices for Fluxion Tool

Client Devices	**Apple iPhone**	**Android Phone**	**Windows Laptop**
User required to reconnect manually to AP after WPA handshake attack.	✗	✗	✗
Device reconnects automatically to AP after WPA handshake attack.	✓	✓	✓
Legitimate AP seen along with Evil-Twin	✗	✓	✓
Able to connect to legitimate AP during rouge AP attack	✗	✗	✗
Captive portal seen.	✓	✓	✓

Based on the above observations in Table 9, it is visible that the Apple iPhone is unable to show the legitimate access point in the available networks, while both the Android Phone and the Windows Laptop can find both the access points.

6.3 Case Study 3: Hak5 Wi-Fi Pineapple Tetra

In this setup, Hak5 Wi-Fi pineapple Tetra was used to create Evil-Twin access points. With the version of v2.4 the Wi-Fi pineapple can create Evil-Twin access points along with providing Internet to the connected clients. The Hak5 Wi-Fi pineapple Tetra does not require the any additional wireless interfaces and the built-in interfaces are by default in the appropriate modes. Furthermore, the default captive portal failed to load in the connected clients. However, additional custom captive portals can be added and deployed. Similarly, by default the Hak5 Wi-Fi pineapple tetra does not generate any OUI information, which the vendor of the chipset used by the wireless adapter. The observation of the performance of Hak5 Wi-Fi pineapple Tetra are recorded in the Table 10.

Table 10: Performance of Hak5 Pineapple Tetra with PineAP

Device	Hak5 Wi-Fi pineapple
Band	2.4GHz and 5GHz
Model	Tetra
Driver	Version 2.4.2
Chipset	Atheros AR9344 and AR9580
Modes Supported	IBSS, Managed, AP, Monitor, P2P-Client, P2P-Go
Setting interface in monitor mode	✗(not required)
Reset Attack on Client	✓
De-authenticating Client	✓
Capturing WPA/WPA2 Handshake	✓
Evil Twin AP creation	✓
Captive portal to steal passwords	✓(deployed additionally)

As observed in the Table 11, after connecting the client devices, it was observed that only the Apple iPhone was unable to see the legitimate access point, while the Android Phone and the windows laptop were able to see both the access points in their available networks. It was also noted that all clients were unable to connect to the legitimate access point during the attack.

Table 11: Observations on Client devices for PineAP

Client Devices	Apple iPhone	Android Phone	Windows Laptop
User response required for WPA handshake attack	✗	✗	✗
legitimate access point seen along with Evil-Twin	✗	✓	✓
Captive portal seen.	✓	✓	✓

6.4 Comparative analysis of the Wi-Fi auditing Tools

The below Table 12 contains the findings from the performance of the tools used to create the Evil-Twin access point with the parameters and specifications outlined in the research methodology.

Table 12: Shows the comparative analysis of the Wireless Auditing Tools

Tools	Airgeddon	Fluxion	PineAP
Type of interface	CLI	CLI	GUI
Capability to provide internet to clients without additional input	✗	✗	✓
Ability to spoof MAC address	✓	✓	✓
Additional adapters required to create Evil-Twin	✗	✓	✗
Ability to perform verification of captured WPA handshake	✗	✓	✗
Number of Captive Portals options	12	78	1(Default 1 but any number can be added)
Ability to add more portals	✗	✗	✓

From these findings, it is evident that PineAP is more robust and can execute complex attacks. Furthermore, it can be used to mount more captive portals without needing additional hardware, while Airgeddon and Fluxion are limited in the number of captive portals they can support.

6.5 Detection Results

Analysis of the information collected by the detection tool clearly indicated the presence of two access points being present. This was observed due to the Vendor specific information parameter able to detect the two distinct Chipset manufacturers creating the access point with the same SSID, where the legitimate access point vendor was Qualcomm Inc. Furthermore, the RSSI values for the legitimate access point were consistent, while the Evil-Twin access points' values were variable. In the setup the legitimate access point consistently remained between the short range of -36 dBm to -48 dBm, whereas the Evil-Twin access point fluctuated from -19 dBm to -40 dBm and even reaching -76 dBm. This proved that the legitimate access point produced a stable signal and the same can be observed in the Figure 5.

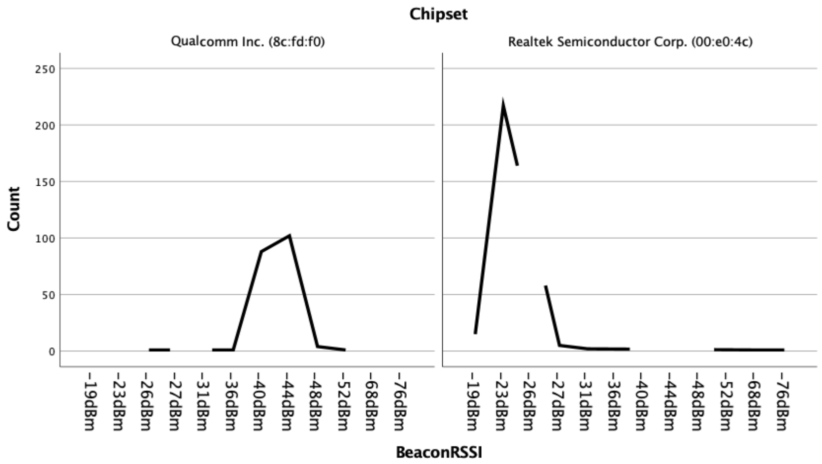


Figure 5: Shows the variation of the signal strength(RSSI) between the legitimate and Evil-Twin access point

Additionally, the sequence numbers of the beacon frames for the legitimate access point remained consistent with a difference of 16, whereas the frame sequence for the Evil-Twin access point was irregular. Furthermore, the time stamp difference between frames was inconsistent for the Evil-Twin access point but not the legitimate one. The Figure 6 shows the Timestamp difference of 102400 between the consecutive beacon frames with a sequence number difference of 16. The Figure 7 shows the inconsistencies in the Timestamp difference between two consecutive frames.

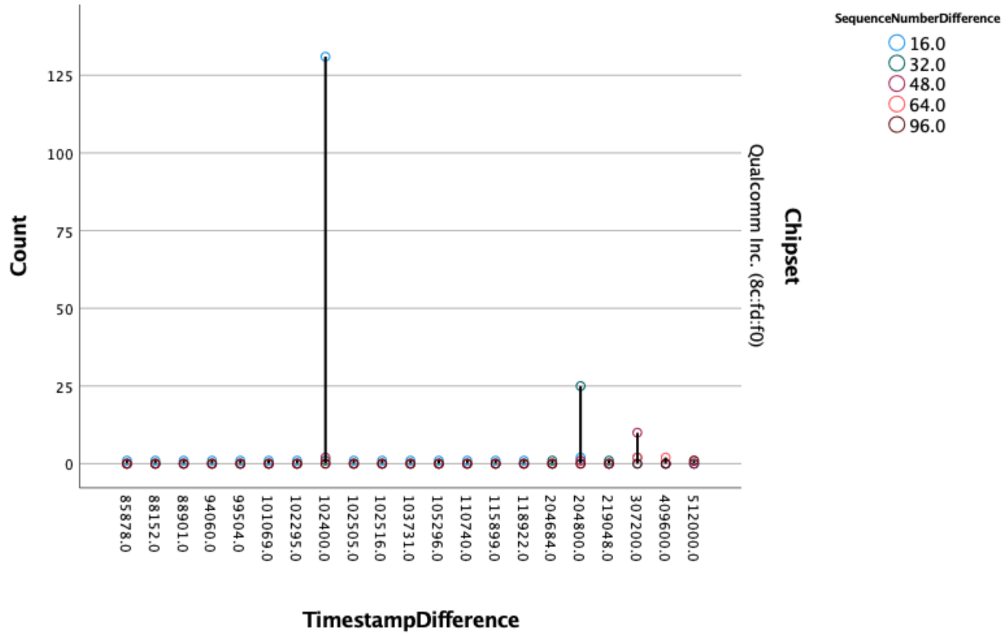


Figure 6: Shows the consistency in the Beacon Frame delay of the legitimate access point

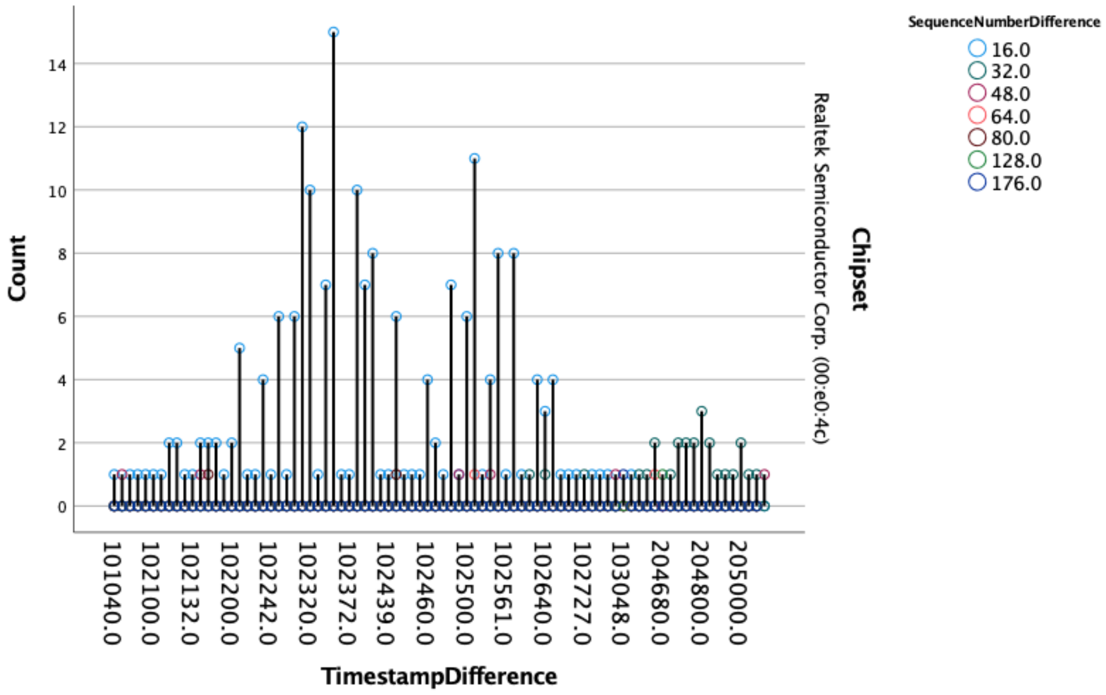


Figure 7: Shows the inconsistency in the Beacon Frame from the Evil-Twin access point

6.6 Discussion

The comprehensive investigation into the Evil-Twin access point was conducted using three distinct case studies. This approach helps test the wireless adapter's capability while simultaneously seeking out potential deficiencies and flaws in the detection tool. Examining and analysing the data from the three case studies enabled the parameters to be narrowed down to accurately detect an Evil-Twin access point. Furthermore, The analysis of the packets from the three cases revealed the following.

- The Vendor-Specific section of a beacon frame packet includes the Vendor OUI (Organizationally Unique Identifier) information that allows us to identify the manufacturer of the chipset used in the access point. Airgeddon and Fluxion do not allow users to modify this, whereas Pineapple Tetra strips this information when creating an Evil-Twin.

- The Group Cipher Suite parameter in the RSN information tag reveals the encryption method of the access point. In contrast, all tools creating Evil-Twin access points do not use encryption.

- Additionally, the Auth Key Management Suite parameter in the RSN information tag displays the authentication method of the access point, which is not used by any of the tools.

- The Frame Control Field in the packet holds the source MAC address information which can be used to identify the vendor. However, when different setups were being tested, some devices that created the access point added random bits of information to the field to create a unique MAC address. As a result of this, the detection tool was not able to look up the MAC address and determine the vendor. Therefore, this parameter was not used to draw the final conclusion.

- The RSSI value under the Radio Tap Header tag provides the signal strength in dBm. This parameter was selected to increase the accuracy of the detection tool as the legitimate access point had a consistent signal strength within a short range. In contrast, the Evil-Twin access point created by the tools had inconsistent signal strength across a wide range.

- Lastly, the timestamps and sequence numbers of the corresponding packets had varying time differences for the Evil-Twin access point. In contrast, the legitimate access point had a consistent difference between each packet.

By analysing the data collected from the three case studies, the presence of an Evil-Twin could be determined by looking at the Vendor OUI and RSSI. Moreover, a definite confirmation was provided by studying the Timestamp, Sequence Number, Cipher, and Suite parameters. These parameters allowed us to discern between the Evil-Twin access point and valid ones.

7 Conclusion and Future Work

The purpose of this research thesis was to develop a more efficient solution by evaluating the available Wi-Fi auditing tools and wireless adapters for Evil-Twin attacks. Results from the analysis displayed that the detection tool could accurately recognize the presence of an Evil-Twin access point. It was noticed that while some of the results provided by the tools were similar, there were also some parameters in which the results showed significant differences. The evaluation results show that the different case studies have successfully met the stated objectives of the research thesis. Based on the above findings, the correct set of parameters was determined to help analyse and detect Evil-Twin access points using beacon-frame delay and wireless network parameter deviation, which will help safeguard users against malicious actors. This research evaluated the various wireless adapters and tools available to create an Evil-Twin access point and determined the combination needed to make it difficult to detect. The evaluation of the three wireless attack tools revealed that the Hak5 Pineapple Tetra is the most user-friendly and robust. Airgeddon is the easiest and most suitable for quick deployment with a single wireless adapter. The evaluation results of the tools helped us identify the parameters such as MAC address can be spoofed using the tools and cannot be used in the detection tool as a parameter to determine the Evil-Twin. The evaluation also shows that the tools cannot change vendor information and be used to detect the presence of the Evil-Twin access point. Also, the encryption and authentication methods are not used while creating Evil-Twin access points by the tools, and an open network is created to perform the attack. Hence, Cipher and Suite information parameters are used in the detection tool to help determine the Evil-Twin access point. It also established the suitable wireless parameters to differentiate between legitimate and Evil-Twin access points and the parameters needed to analyse and detect them. The results from this research indicate that there is room for further improvement.

For future work on this research paper, the following can be considered. When conducting the research and making the case studies, it was assumed that the attacker had deceived the client devices into connecting to the Evil-Twin access point. The captive portal was not intended to imitate a particular organization. To better identify and detect these Evil-Twin access points, research into the social engineering aspect of this attack can be undertaken. This can start with surveying the building to locate the access points present and creating a heat map of the environment's wireless network using software such as jwaves.io. After setting up the Evil-Twin access point, deploying a targeted captive portal and recording the participants' behaviour is the next step. Analysing the gathered data, making conclusions on the attack's effectiveness, and finding ways to better identify these Evil-Twin access points should follow.

Furthermore, the results of this experiment could help create an awareness campaign to inform people about the risks of connecting to unknown Wi-Fi networks. This approach would allow for a more comprehensive understanding of the Evil-Twin attack while being more creative and innovative. The method used in the research to detect the Evil-Twin access point was the passive method. The detection tool was not connected to the Evil-Twin access point, thus limiting the parameters that can be evaluated. The active method can also be used to examine the environment for unauthorized or suspicious access points. By combining different approaches, a hybrid detection tool can be built to consider more metrics for comparison, such as the Maximum Common Subsequence index. This would increase the accuracy of the detection tool.

References

‘2017-norton-wifi-risk-report-global-results-summary-en.pdf’ (no date). Available at: https://primo-europe.eu/wp-content/uploads/2017/07/2017-norton-wifi-risk-report-global-results-summary-en.pdf (Accessed: 14 December 2022).

Alotaibi, B. and Elleithy, K. (2015) ‘An empirical fingerprint framework to detect Rogue Access Points’, in *2015 Long Island Systems, Applications and Technology. 2015 Long Island Systems, Applications and Technology*, pp. 1–7. Available at: https://doi.org/10.1109/LISAT.2015.7160206.

Amoordon, A. *et al.* (2022) ‘A Threshold-Based Detection Approach To Detect Fake Access Points and Jamming Attacks on IEEE 802.11 Networks: Implementation, Results and Limitations’, in *2022 3rd URSI Atlantic and Asia Pacific Radio Science Meeting (AT-AP-RASC). 2022 3rd URSI Atlantic and Asia Pacific Radio Science Meeting (AT-AP-RASC)*, pp. 1–4. Available at: https://doi.org/10.23919/AT-AP-RASC54737.2022.9814377.

Anmulwar, S. *et al.* (2014) ‘Rogue access point detection methods: A review’, in *International Conference on Information Communication and Embedded Systems (ICICES2014). International Conference on Information Communication and Embedded Systems (ICICES2014)*, pp. 1–6. Available at: https://doi.org/10.1109/ICICES.2014.7034106.

Asaduzzaman, Md., Majib, M.S. and Rahman, Md.M. (2020) ‘Wi-Fi Frame Classification and Feature Selection Analysis in Detecting Evil Twin Attack’, in *2020 IEEE Region 10 Symposium (TENSYMP). 2020 IEEE Region 10 Symposium (TENSYMP)*, pp. 1704–1707. Available at: https://doi.org/10.1109/TENSYMP50017.2020.9231042.

Burns, A. *et al.* (2017) ‘A Novel Traceroute-Based Detection Scheme for Wi-Fi Evil Twin Attacks’, in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference. GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pp. 1–6. Available at: https://doi.org/10.1109/GLOCOM.2017.8253957.

Jadhav, S., Vanjale, S.B. and Mane, P.B. (2014) ‘Illegal Access Point detection using clock skews method in wireless LAN’, in *2014 International Conference on Computing for Sustainable Global Development (INDIACom). 2014 International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 724–729. Available at: https://doi.org/10.1109/IndiaCom.2014.6828057.

Jang, R. *et al.* (2020) ‘Catch Me If You Can: Rogue Access Point Detection Using Intentional Channel Interference’, *IEEE Transactions on Mobile Computing*, 19(5), pp. 1056–1071. Available at: https://doi.org/10.1109/TMC.2019.2903052.

Kao, K.F. *et al.* (2014) ‘An Accurate Fake Access Point Detection Method Based on Deviation of Beacon Time Interval’, in *2014 IEEE Eighth International Conference on Software Security and Reliability-Companion. 2014 IEEE Eighth International Conference on Software Security and Reliability-Companion*, pp. 1–2. Available at: https://doi.org/10.1109/SERE-C.2014.13.

Ketkhaw, A. and Thipchaksurar, S. (2017) ‘Hidden Rogue Access Point Detection Technique for Wireless Local Area Networks’, in *2017 21st International Computer Science and Engineering Conference (ICSEC). 2017 21st International Computer Science and*

Engineering Conference (ICSEC), pp. 1–5. Available at: https://doi.org/10.1109/ICSEC.2017.8443803.

Kitisriworapan, S., Jansang, A. and Phonphoem, A. (2019) 'Evil-Twin Detection on Client-side', in *2019 16th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). 2019 16th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pp. 697–700. Available at: https://doi.org/10.1109/ECTI-CON47248.2019.8955158.

Lanze, F. *et al.* (2015) 'Hacker's toolbox: Detecting software-based 802.11 evil twin access points', in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC). 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 225–232. Available at: https://doi.org/10.1109/CCNC.2015.7157981.

Lotfy, Y. *et al.* (2021) 'Privacy Issues of Public Wi-Fi Networks', in, pp. 656–665. Available at: https://doi.org/10.1007/978-3-030-76346-6_58.

Lovinger, N. *et al.* (2020) 'Detection of wireless fake access points', in *2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 113–118. Available at: https://doi.org/10.1109/ICUMT51630.2020.9222455.

Mwinuka, L.J. *et al.* (2022) 'FakeAP Detector: An Android-Based Client-Side Application for Detecting Wi-Fi Hotspot Spoofing', *IEEE Access*, 10, pp. 13611–13623. Available at: https://doi.org/10.1109/ACCESS.2022.3146802.

Nakhila, O. and Zou, C. (2016) 'User-side Wi-Fi evil twin attack detection using random wireless channel monitoring', in *MILCOM 2016 - 2016 IEEE Military Communications Conference. MILCOM 2016 - 2016 IEEE Military Communications Conference*, pp. 1243–1248. Available at: https://doi.org/10.1109/MILCOM.2016.7795501.

Vanjale, S. and Mane, P.B. (2014) 'A novel approach for elimination of rogue access point in wireless network', in *2014 Annual IEEE India Conference (INDICON). 2014 Annual IEEE India Conference (INDICON)*, pp. 1–4. Available at: https://doi.org/10.1109/INDICON.2014.7030418.

Wi-Fi® predictions from Cisco's Annual Internet Report | Wi-Fi Alliance (2020). Available at: https://www.wi-fi.org/beacon/the-beacon/wi-fi-predictions-from-cisco-s-annual-internet-report (Accessed: 13 December 2022).

Yang, C., Song, Y. and Gu, G. (2012) 'Active User-Side Evil Twin Access Point Detection Using Statistical Techniques', *IEEE Transactions on Information Forensics and Security*, 7(5), pp. 1638–1651. Available at: https://doi.org/10.1109/TIFS.2012.2207383.

Zhang, Z. *et al.* (2020) 'Rogue AP Detection using Similarity of Backbone Delay Fluctuation Histogram', in *2020 International Conference on Information Networking (ICOIN). 2020 International Conference on Information Networking (ICOIN)*, pp. 239–244. Available at: https://doi.org/10.1109/ICOIN48656.2020.9016480.