Design and Implementation of a PacketXtract Forensic Tool

GRADUATE PROJECT REPORT

Submitted to the Faculty of
Department of Computing Sciences
Texas A&M University-Corpus Christi
Corpus Christi, Texas

In Partial Fulfillment of Requirements for the Degree of
Masters of Science in Computer Science

By

Bharath Kumar Paravastu
Fall 2010

Committee Members

Dr. Mario Garcia
Committee Chairperson

Dr. David Thomas
Committee Member

Dr. Hongyu Guo
Committee Member
ABSTRACT

Wireless access is considered as the preferred choice of connecting to the internet in the modern networking era. Wireless digital security forensics is now regarded as a major challenge to both technical and legal organizations. The rapid growth in wireless networks and access points have created more security vulnerabilities and posed a major challenge to both organizations and consumers. There are various freeware packet sniffing tools available which are capable of listening and analyzing the network traffic. Wireshark is one of the most popularly used packet sniffing tool capable of doing this work. Wireshark uses Winpcap library to analyze and listen the traffic.

This project mainly discusses about the various wireless forensics tools available for both Linux and Windows environments. The test cases for generation and forensic analysis of these attacks is presented. Various test cases on packet sniffers capable of listening and analyzing the traffic is presented. This project mainly focuses on implementing a packet sniffer that is similar to Wireshark. It is similar in functionality to Wireshark, but it uses socket programming. The main advantage of using this socket is that they have core network functionality and can run on any hardware out of the box.
# TABLE OF CONTENTS

Abstract.................................................................................................................................................. ii

Table of Contents.................................................................................................................................... iii

List of Tables........................................................................................................................................... iv

List of Figures.......................................................................................................................................... iv

1. Background and Rationale.................................................................................................................... 1
   1.1 Discovering Wireless Networks........................................................................................................ 1
   1.2 Tracing Wireless Hackers................................................................................................................ 2
   1.3 Existing Tracing Technologies........................................................................................................ 3
   1.4 Forensic Data Collection on Wireless Network Environment....................................................... 4

2. Narrative............................................................................................................................................ 6
   2.1 Wireless Security.............................................................................................................................. 6
   2.2 Wireless Forensics.......................................................................................................................... 12
      2.2.1 Techniques used in Intruder Detection.................................................................................... 13
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure Number</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Laptop connected to a directional antenna</td>
<td>2</td>
</tr>
<tr>
<td>1.2</td>
<td>Triangulation using multiple access points</td>
<td>3</td>
</tr>
<tr>
<td>2.1</td>
<td>WLAN Devices and Systems</td>
<td>12</td>
</tr>
<tr>
<td>2.2</td>
<td>Triangulation using three access points</td>
<td>14</td>
</tr>
<tr>
<td>2.3</td>
<td>Omni-directional Triangulation</td>
<td>14</td>
</tr>
<tr>
<td>2.4</td>
<td>Wireless Grid</td>
<td>15</td>
</tr>
<tr>
<td>2.5</td>
<td>IP Header Format</td>
<td>21</td>
</tr>
<tr>
<td>2.6</td>
<td>TCP header format</td>
<td>22</td>
</tr>
<tr>
<td>2.7</td>
<td>UDP header format</td>
<td>22</td>
</tr>
<tr>
<td>2.8</td>
<td>CurrPorts</td>
<td>25</td>
</tr>
<tr>
<td>2.9</td>
<td>SmartSniff capturing window</td>
<td>27</td>
</tr>
<tr>
<td>2.10</td>
<td>Capturing options in Smart Sniff</td>
<td>27</td>
</tr>
<tr>
<td>2.11</td>
<td>Capturing with WinPcap Capture driver</td>
<td>28</td>
</tr>
<tr>
<td>2.12</td>
<td>Adapter Watch</td>
<td>28</td>
</tr>
<tr>
<td>2.13</td>
<td>PingInfo View</td>
<td>29</td>
</tr>
</tbody>
</table>
Figure 4.8 Spoofing the current MAC to Faked MAC.............................................. 43
Figure 4.9 Successful MAC address spoofing............................................................ 43
Figure 4.10 Wi-Fi brought down to normal mode..................................................... 44
Figure 4.11 Connecting to the public unsecured network......................................... 44
Figure 4.12 Checking the access to internet in public unsecured network............... 45
Figure 4.13 Attacker gaining access to internet......................................................... 45
Figure 4.14 Packet capturing in Wireshark................................................................. 46
Figure 4.15 Http filtering in Wireshark.......................................................... 47
Figure 4.16 Display filters in Wireshark........................................................................ 47
Figure 4.17 Http filter.............................................................................................. 48
Figure 4.18 Wi-Fi in monitor mode............................................................................. 49
Figure 4.19 Initial output........................................................................................... 50
Figure 4.20 Testing injections of packets................................................................. 50
Figure 4.21 Successful working of packet injection.................................................. 51
Figure 4.22 Gathering packets/data for cracking key.............................................. 51
Figure 4.23 Capturing ARP requests........................................................................ 51
Figure 4.24 Air crack initialization ................................................................. 52
Figure 4.25 Air crack process .................................................................... 53
Figure 4.26 Cracked password key ............................................................... 53
Figure 4.27 Running Kismet ...................................................................... 54
Figure 4.28 Running Kismet (Contd...) ....................................................... 55
Figure 4.29 Running Kismet as root ............................................................ 55
Figure 4.30 Startup options in Kismet ....................................................... 56
Figure 4.31 Adding interface to wireless card ........................................... 57
Figure 4.32 Entering wireless card name in kismet ................................. 58
Figure 4.33 BSSID/MAC address ............................................................... 58
Figure 4.34 Client list .......................................................... .......................... 59
Figure 4.35 Open console .......................................................... ........................ 60
Figure 4.36 Captured data in open console .............................................. 60
Figure 4.37 Finding file starting with kismet and ending with .pcdump ........ 61
Figure 4.38 Pressing key F3 .......................................................... .......................... 61
Figure 4.39 Searching string like .com ................................................................. 62
Figure 4.40 Repeated searching .......................................................... 62
Figure 4.41 Setting Wi-Fi to monitor mode ........................................... 63
Figure 4.42 DOS attack on channel 5 .................................................. 64
Figure 4.43 DOS de-authentication attack ........................................ 64
Figure 4.44 Authentication DOS mode ............................................. 65
Figure 4.45 Third DOS de-authentication attack .................................. 65
Figure 4.46 Listening to the packets .................................................. 66
Figure 4.47 Analysis of the packets captured ...................................... 67
Figure 4.48 Wireshark – Listening of the packets .................................. 68
Figure 4.49 Wireshark – Analysis ...................................................... 68
Figure 4.50 Tcpdump – Listening to packets ....................................... 69
Figure 4.51 PLAB – Listening to packets ............................................ 70
Figure 4.52 Network Miner – Listening to packets .............................. 71
Figure 4.53 Colasoft Capsa 8 – Listening to the Packets ..................... 72
LIST OF TABLES

Table 2.1 WLAN protection main methods ...................................................... 10
1. BACKGROUND AND RATIONALE

This section gives background and a brief ground work on wireless forensics. Wireless forensics is an evolving challenge to network forensics. Network forensics typically involves the gathering, documenting, and analyzing of legal charges being brought before a judge in court. Key forensic information can provide evidence to the potential origin of the intruder in the event of legal charges being brought before the judge in court. Wireless forensics is a relatively new concept, but with the continued popularity of increased mobility provided by wireless computing and connectivity, the parallel growth of wireless cyber crime also continues to increase day-by-day. Even though wireless forensics is a form of network forensics, the methods used to obtain information flow over a wireless network are different and often become quite challenging. So this basic idea made this research to progress in this field. [Achi 2009].

In wireless network the Communication between the wireless device and the wireless access point is simple. When network packets are exchanged between the device and the access point association is said to be established. In some situations, the associations will only occur when the MAC address of the wireless device matches to the MAC address stored in the access point. In some situations the association is established by PSK (Pre-Shared Key) or by using any of the encryption standards. Thus, when network traffic exchanged between the device and the access point, the wireless forensics laptop in the network can determine the network statistics. Thus, this forensics laptop is used to determine the various associated devices, link them to the access point. This brief background discusses the techniques adopted by various intruders in locating the wireless network. It also discusses the challenges faced by the forensics investigator in locating the wireless intruder and also the existing tracing technologies [Achi 2009].

1.1 Discovering Wireless Networks

Active scanning and Radio-Frequency Monitoring (RF – MONT) are the two methods in discovering the wireless networks. In active scanning the hacker sends the probe request and waits for the probe response from the wireless network. This mechanism is not effective in hacker’s perspective. Active scanning is similar to that of pinging a system. In this mechanism the hacker knows that the system exists, but the system has no idea about the existence of the hacker. Netstumbler uses active scanning. In radio frequency monitoring the hacker listens to the
radio frequencies that the wireless network operating on. In radio frequency monitoring, communication between the access point and the client is screened. Not all the wireless cards support radio frequency monitoring. Only wireless cards with a prism based chipset or the derivative of the chipset with its own specification can be used. It becomes easy for the intruder to detect the network, but becomes difficult for the investigator to trace back the hacker [Velasco 2007].

1.2. Tracing Wireless Hackers

Tracing wireless hackers in wireless connection is a difficult task. In wired connection users have their own ISP (Internet Service Provider). So it becomes simple to trace back the hacker with ISP. In the case of wireless connection the hacker is present close to the access point about a few miles. The hacker can be determined on the basis of equipment they use, interference around them and thickness of the wall. In the wireless network, the hacker may use the IP of some other person in the network. The hacker may use either Omni directional antennas or directional antennas to detect the wireless network [Velasco 2007].

Omni-directional antenna uses the circular pattern which spread in all directions and this is not a good idea for the hacker. If directional antenna is used the narrow beam is sent in a specific direction. A smart hacker uses directional antenna. It spreads a narrow beam in a specific direction. Figure 1.1 shows an attacker connected to a directional antenna.

![Figure 1.1 Laptop connected to a directional antenna [Velasco 2007]](image-url)
1.3. Existing Tracing Technologies

Global positioning systems are used in tracing the intruders. But these GPS are not effective in indoors. The signals of GPS can be blocked inside a building and effective readings cannot be established. Three techniques are now used in tracing the intruder. They are the closest access point, triangulation and radio-frequency finger printing. Closest access point is simple and least accurate. In closest access point, the method assumes that the user is within the range of the access point. The network administrator locates the user by the access point that is associated with. The main drawback is the assumption that the user is located within the range of the access point. In some cases the hacker might use a directional antenna, so the location of the user is located outside the access point transmission [Velasco 2007].

Triangulation provides better accuracy compared to closest access point. In triangulation, several access points are placed in different locations. In order to locate a device the access point is queried to see if it can read the signal from the wireless device. The locating system then keeps track of the signal strength from each of the access points, and then a circle is drawn around each of the access points with signal strength as radius. The stronger the signal, the closer the device to the access point. The information is then triangulated to know the exact position of the device. The main disadvantage of triangulation is that it does not consider the effect of environment on signal strength. Figure 1.2 shows location tracking of a device using three access points [Velasco 2007].

![Figure1.2 Triangulation using multiple access points [Velasco 2007]](image-url)
RF finger printing is similar to triangulation. In RF finger printing several access points are placed in different locations. In RF fingerprinting, RSSI (Radio Signal Strength Indication) values are taken at specified locations. These RSSI values are fed into the database. The RSSI values taken from the access point and compared with the values stored in the database. From this comparison the location of the wireless device can be found [Velasco 2007]. A detailed explanation of these techniques is described in the section 2.

1.4. Forensic Data Collection on Wireless Network Environment

The major problem with the wireless networks is the lack of a physical footprint. There is one major underlying issue with the collection and analysis of the data in the Wireless Network. There is a possibility that an investigator is not sure about the existence of a suspected computer in the scene. The only way to get the true evidence is to identify all the wireless devices that are a source of potential evidence. After the identification, the wireless spectrum and the protocols are analyzed to trace back the potential evidence. So, based on this information, the investigator may have the idea whether the wireless network should be physically searched. It also gives the information regarding the number of devices in the network and information regarding uniquely identifiable MAC address [Turnbull 2008].

The unique characteristics of the wireless devices use some special approach in locating the wireless devices in search-and-seizure environment. Since, the wireless devices are still in use or remotely accessible they cannot be identified in plain sight. Live analysis can be conducted by using the commercial-off-the-shelf software or open source software. Wireless networks that are present in a given area and the count of number of devices in the network and details of each of the network can be known by conducting the live analysis. The potential evidence can be identified by performing live forensics analysis and using advanced technologies [Turnbull 2008].

Using live network mechanism for identifying the potential source of digital evidence is not the forensics expert function. The identification of the devices is very much critical for the forensics analysis. The forensics experts must work very much close with the network administrators, the intrusion detection specialists and the risk assessment analysis team. The live
data interception that is the part of the intelligence role plays an important role in live network mechanism [Turnbull 2008].

Passive network discovery tools such as Kismet or Kismac shows all the information about the wireless networks in within a specified range. This also gives the information regarding the SSID (Service Set Identifier), MAC address, and also the appropriate physical location of the wireless device. The tools can be used by the forensics investigator to collect all the raw wireless frames and interpret the results. The tools display some of the collected data on-screen and other information is stored into files. A copy of raw data is still stored for further forensics analysis. The drawback in the current live analysis is that it is unable to indicate the characteristics of network topology that has been misused [Turnbull 2008].

Live analysis is very much difficult to implement. It has to be conducted when the streams are active. Live analysis is conducted when the communication is still occurring. The analysis that has been conducted needs continual revision. As live analysis can be conducted after the completion of the entire communication to get better results, it has the major drawback of being less than real time. As more communication is occurring, the applicability of the live analysis is constantly revised. But sometimes it leads to false assumptions. The time frame given to read and analyze the information is very much small in live analysis. Analysis without a time frame can read and analyze each of the received packets. It analyzes the packets with relation to the previous communication. As a result it can interpret the communication beyond the simple mechanisms such as port and connection type [Turnbull 2008].

The encryption key for a given network can be inferred with live analysis. It can be inferred if some particular protocols are used and if there is sufficient traffic between the wireless components. The traffic analysis cannot be completely performed until the encryption key is available. The encryption key can be either obtained from inference or from the device through postmortem analysis. The underlying assumption in wireless differs from wired equivalents. From analysis of different OSI layers the information regarding the individual devices can be obtained [Turnbull 2008].
Telecommunication interception systems can be used for postmortem analysis. In 802.11 based wireless networking, the postmortem analysis can be used to further determine the 802.11 based networks or devices for further evidence. The telecommunication interception systems can also be used to analyze the information regarding the previous connection of the 802.11 based networks and also searching the evidence regarding the misuse [Turnbull 2008].

2. NARRATIVE

2.1 Wireless Security

Wireless technology has been gaining rapid popularity for some years. The contrast between the wireless usage and the security standards shows that the security standards are not growing up with the increasing wireless usage. The wireless security standard that is adapted depends on the level of security that it provides and also on ease of use. Three major security standards are presently adapted. They are the WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protection Access) and WPA2/802.11i (Wi-Fi Protection Access, Version2) [Lashkari 2009].

The WEP is designed to provide security in a wired network by using an RC4 algorithm. It is used to provide security from sender to receiver and vice versa, thus it provides security on two sides of data communication. WEP uses four steps to encrypt the data. In the first step the secret key (40-bit long) is combined with an initialization vector to form an encryption or decryption key. This key acts as an input to the pseudo-random number generation algorithm. In the third step the plain text performs an integrity check to get the ICV (Integrity Check Value) which acts as an input to the RC4 algorithm. In the fourth step the key sequence and the ICV acts as an input to the RC4 algorithm to produce the cipher text by attaching IV (Initialization Vector) in the front of the cipher text [Lashkari 2009].

RC4 uses five different operations to decrypt the received sided communication. In the first step pre-shared key and the IV are concatenated to form a secret key. The cipher text and secret key are the input to the RC4 algorithm. In the third step the ICV and the plain text are separated. The plain text is sent to an integrity algorithm to produce a new ICV. The new ICV is then compared with the original ICV. In this, WEP is used to perform encryption for secure transmission. WEP2 is an advanced version of WEP designed in order to stop the brute-force
key attacks. In WEP2, the key values and the IV are increased to 128 bits. In order to overcome weak IV’s WEP+ was designed by the agree systems. Although it provides better security, there are some attacks against WEP+. The WEP + cannot prevent replay attacks. Dynamic WEP changes the WEP keys dynamically. It is vendor-specific feature provided by several vendors such as 3Com. This dynamic behavior of the WEP keys made WEP as an integral part of TKIP (Temporal Key Integrity Protocol) [Lashkari 2009].

WEP has serious weaknesses

- WEP cannot prevent the forgery of the packets.
- WEP cannot prevent replay attacks. An attacker can easily notice a packet and resend a packet which will be accepted as legitimate.
- WEP does not use the RC4 algorithm properly. The keys are easily subjected to brute-force attacks.
- WEP uses the same IV after a particular time. Key management is very poor and also updating the key is poor [Lashkari 2009].

Improved data encryption (TKIP), user authentication and Integrity are the improvements that can be made in WEP.

WPA personal or WPA commercial has come as an improvement over WEP. WPA is similar to that of WEP and specifies two different operations.

- WPA personal uses a pre-shared key for small office and home authentication. WPA personal does not use an authentication server. The data cryptography key in WPA can go up to 256 bits. The pre-shared key is used to establish the initial session with the access point. Both the client and the access point already posses the pre-shared key. WPA provides mutual authentication by using the pre-shared key without an authentication server.
- The enterprise WPA or commercial WPA uses an authentication server 802.1x. This authentication server provides excellent control and security to the users in the wireless network. WPA uses 802.1 x and EAP (Extended Authentication Protocol) for authentication and uses advanced TKIP (Temporal Key Integrity Protocol) for
encryption purposes. Here pre-shared key is not used, but instead RADIUS server is used here. 802.1X and EAP provide many benefits such as integration with windows login process and also support EAP-TLS and also PEAP authentication methods [Lashkari 2009].

The main reason WPA has been designed after WEP is because of the complex encryption that it uses on TKIP protocol. In order to avoid the bit-flipping attacks the WPA is also associated with MIC (Message Integrity Check). The MIC is applied to the WEP by hashing technique. The encryption in TKIP is similar to RC4, but with slight difference. The duplication of the IV is made and the copy is sent to the next step and the other IV copy is hashed with the base key to produce the special key. This hashing results lead in the improvement of the RC4 algorithm. The result of RC4 algorithm is a sequential key. This sequential key is XORed with the plain text to produce the encrypted message. WPA has many advantages compared to WEP [Lashkari 2009].

- A cryptographic message integrity code called MIC to handle all the forgeries in the wireless network.
- A new initial vector sequencing discipline to remove all the replay attacks from attackers.
- A per-packet key mixing function which is used to separate the weak IV’S from the weak keys.
- A rekeying mechanism is used to provide better encryption and provides integrity in keys, minimizing the attacks that emerge out from key reuse.

There are vulnerabilities in WPA-PSK networks. These vulnerabilities are based on PMK (Pairwise Master Key). PMK is the concatenation of the SSID (Service Set Identifier), length of the SSID, pass-phrase and nonce. The nonce represents the number of bit streams used in each session. This key is transmitted in the normal traffic and can be easily obtainable. PTK (Pair wise Transient Key) is a re-keyed HMAC function on PMK. If four handshake signals are captured, the pass-phrase of PMK can be easily subjected to dictionary attacks. If the key is generated from the pass-phrase of more than 20 characters it is likely to resist the dictionary attacks [Moskowitz 2003].
WPA cracker was released to break down the WPA protected network. In Linux systems cowpatty is used to perform brute force attacks. The shared pass-phrase can be determined by performing the brute force attacks. These two attacks require the attacker to supply the dictionary file and the four way handshake. The four way handshake is supplied in a dump file. The difference between both of these is that the WPA requires the attacker to supply the string. In cowpatty automatic parser is used to generate the required string [Miller 2001].

WPA2 and 802.11i standards are often terms used interchangeably. 802.11i and WPA2 are not just the future of wireless access authentication, but they are the future of wireless access. WPA is associated with several limitations. WPA2 is designed as a future proof solutions based on the lessons learnt from WEP and WPA standards. Motorola is the key behind the WPA2 standard and it provides next generation products based on this standard. WPA2 standard is durable for many reasons. The first is because of the encryption algorithm that it uses. The NIST (National Institute of Standards and Technology) has designated that the successor of the Data Encryption Standard is the Advanced Encryption Standard (AES) [Miller 2001].

WPA2 like WPA supports two different modes of security. They are for home and corporate networks. In home mode security both the users and the access points store the secret key whose length is up to 64 ASCII characters. This key is entered manually in both the user system and the access point to provide authentication. WPA2 in home mode provides the same security problems as in WEP and WPA-PSK. The corporate security is based on 802.1X, the EAP authentication frame work such as RADIUS (Remote Authentication Dial-in User Service), EAP types such as EAP-TLS to provide stronger authentication and secure key distribution. In 802.11i the key for secure authentication is allowing for client distribution, wireless network authentication, key distribution and pre-authentication. When using 802.1X along with 802.1i, it is suggested using EAP-TLS for authentication between the wireless client and the wireless access point [Miller 2001].

RADIUS stands for Remote Authentication Dial in User Service. This protocol is used to provide centralized Authentication, Authorization and Accounting (AAA). As the number of dial-up users increases the burden on NAS (Network Access Server) increases. Username, password and key management becomes difficult. Because of ubiquitous nature offered by the RADIUS server, it is used by many ISP and enterprises to manage the internet and internal
networks. In RADIUS authentication, NAS operates as a RADIUS client. This client is responsible for sending the user information to the RADIUS server and also implementing the response sent by the server. RADIUS server is responsible for receiving the user connection information, distinguishing the users and sending the configuration information to the client. RADIUS is a client/server protocol that runs in the application layer of the OSI model. All the transactions between the client and the server are identified by the shared secret key. This shared secret is not known to the network before. All the usernames, passwords are transmitted in encrypted form between the client and the server to avoid eavesdropping [Miller 2001].

In 802.1X, the major drawback is the beacon packets and probe request/response packets cannot be protected. The attacker can also perform denial of service attacks. The attacker can identify the wireless clients based on hardware MAC address of client. 802.1 X contains three major components. They are the supplicant, authenticator and the authentication server. The supplicant (Wireless Client) initially connects to the Authenticator (Access Point). Once this link has been established the supplicant can authenticate using this link and used for further authentication [Miller 2001].

Here table 2.1 explains the differences between the WEP, WPA, WPA2, 802.1X and VPN security standards. It explains the main features of the security standard, their advantages and shortcomings.

Table 2.1 WLAN protection main methods [Miller 2001]
The shortcomings in the IEEE 802.11 lie in both the encryption and authentication. In open system authentication the access point constantly sends out the beacon frames to show its presence. These frames contain the SSID of the network. So an attacker can easily accept these frames and then use these to gain access to the access point. Some systems do not allow the SSID beaconing so that SSID cannot be transmitted. But it creates several problems in hand-offs. In Shared Key Authentication brute force attack or standard dictionary attack can be used to break into the network. WEP uses a very short key and if the initialization vector of two packets can be determined, simply XOR ing the encrypted texts will result in determining the original texts, thus the original texts can be recovered. Vulnerabilities of the original IEEE 802.11 is also found in the case of MAC address filtering mechanism. MAC addresses represent the physical address of the system. Because of the growing number of users, attacks based on MAC addresses filtering are now a hot spot. As new users add on and the old users leave on it requires a constant attention on updating the MAC addresses on access points. If it is not done it imposes several security concerns. WEP2 was found to more insecure than WEP. InWEP2 increasing the key size to 128 bits does not lead to the collisions. Dictionary attacks were possible through the use of Kerberos-authentication systems. Certain types of attacks cannot be prevented by the dynamic WEP. Although the IV problem can be solved by the Dynamic WEP still it offers a partial solution to all the wireless security problems. As this offer only a partial solution dynamic WEP has never been implemented worldwide. There are also many security concerns in the WAP, i.e., Wireless Application Protocol [Miller 2001].

There are many growing technologies that require more research and also great challenges to be addressed. In Wireless Mesh Networks, the main challenge in this technology is its complexity. The general logic behind this is the routers exchanging the packets to the desired destination. This technology is used both for broad band Internet access, WLAN and WMN. WMN, which supports user mobility, must be fast adaptable to the changing frequencies and fading. But unfortunately the physical layer is not reliable. The major challenges in this field lies in the link adaption, multiple transceivers, directional antennas and link quality feedback [Miller 2001].
2.2 WIRELESS FORENSICS

Figure 2.1 WLAN devices and systems [Achi 2009].

Figure 2.1 show different devices and systems connected in a Wireless Local Area Network. Wireless networks offer many advantages over wired network. The advantage of the wireless networks is the price. Wireless networks offer less security compared to wired networks. In the wireless network, the intruder or the hacker can illegally enter into the network and may harm the network. So the security of the wireless network is compromised. With the growing number of wireless networks and wireless access devices, the security is getting compromised. With the increasing security vulnerabilities, techniques and tools have to be developed that tries to counteract these vulnerabilities. Once the wireless network gets attacked, it becomes difficult for the forensics investigator to trace back or detect the intruder or the hacker. Three different locating tracking techniques the closest access point, the triangulation, the Radio Frequency Fingerprinting are used to trace back the hacker [Achi 2008].

The various security vulnerabilities have forced the administrators to protect the wireless networks from malicious activities. The administrators use security forensics to secure their wireless networks from intruders or hackers. The Law Enforcement Agencies (LEA) has developed strict rules to secure their wireless networks from malicious activities. This agency is associated with several technical and legal challenges. The main part in the forensics investigation is the collection of evidence and submitting it to the court. Different tools are used by the forensics investigators in collecting the digital evidence. Different standards are used by various organizations in submitting the evidence to the court. Since the digital evidence is
processed by the various forensics tools. This digital evidence is subject to third part legal and technical experts. If the digital evidence gets manipulated it gets rejected by the court [Achi 2009].

A Lot of work has been focused on collecting and analyzing the digital evidence. This is performed after a security breach has been performed on a network. After a security breach has taken place, digital forensics focused on collecting and analyzing the digital evidence. This is an emerging area of research and still much more research has to be concentrated in this area. Digital forensics has been emerging from the day the devices such as PDA, laptops and cell phones have become part of the life [Achi 2009].

2.2.1. Techniques used in Intruder Detection

Three major techniques for intrusion detection are the closest access point, the triangulation and Radio Frequency Fingerprinting (RF Fingerprinting).

In the closest access point technique, the access point to which the user is associated with is determined. Once the access point is determined, the next step is to trace the hacker. The access point might be transmitting in directional or Omni –directional (in all directions). So the hacker must be within that range of transmission. So, the hacker can easily be determined. But if the hacker uses directional antenna, the attacker will be present outside the network. It makes it difficult to identify the identity of the hacker. According to the closest access point the hacker must be present within the range of the access point transmission. But this is misleading if the hacker uses directional antenna, as there is no need for the hacker to be within the range of the access point transmission [Achi 2008].

In triangulation, access points are placed throughout the network. All the access point that receives the device transmission is spotted. The access points that receive the stronger transmission from the device are closest to the device. The signal strength received by all the access points for that particular device is noted. This information is sent to the locating system that is used to identify the device. With the signal strength received as radius, a circle is drawn around each of the access point. The greater the signal strength the less is the distance between the point and the device. If the access point receives stronger signal strength, then the device is
located within that transmission of the access point. The stronger the signal strength the smaller the size of the circle around the access point [Achi 2008].

Figure 2.2 Triangulation using three access points [Achi 2008]

Figure 2.2 shows locating the intruder using the three access points. Three circles are drawn around each of the access points. If the signal strength is higher, the radius of the circle is lower. The intersection of all the circles might probably give in the location of the hacker. The triangulation has some severe disadvantages. The signal strength is altered by the environmental condition. The signal strength received by the access point might be altered. The triangulation approaches assumes that signal strength is transmitted equally in all the directions. This might lead in false miscalculations and incorrect location of the intruder. Figure 2.3 shows Omni directional triangulation.

Figure 2.3 Omni-directional triangulation[Achi 2008]

In order to overcome the limitations in triangulation an alternate method is presented. In this method, the access points are scattered throughout wireless network. The signal strength
received by the wireless device is taken from multiple locations. To improve the accuracy, the signal strength received by the wireless access point is taken from one location and then moved to different location. The received signal strength is calculated at different locations. The signal strength received depends on many other factors, such as thickness of the wall present between the wireless access point and the device, environment conditions, the objects present between the device and access points. The attackers always prefer to stay away from the network. They try to use directional antennas to get connected to the network. The larger is the distance of the attacker from the network, the difficult to trace the hacker. To improve the accuracy, the access points must be present outside the network to eliminate the concept of interference [Achi 2008].

Wireless Grids is a technique used to locate intruder in a wireless network. The dark points in the Wireless Grid represent the access points and the circles around the dark point’s shows the signal strength. This looks similar to that of triangulation. But the access points are scattered throughout the network. The location system is invoked to calculate the RSSI (Received Signal Strength Indication) values at different locations. The RSSI values are fed into the database. These RSSI values are called RF fingerprints. RF fingerprinting shows better performance compared to other techniques. RADAR can be used to calculate the effectiveness of RF fingerprinting techniques in a building [Achi 2008]. Figure 2.4 shows Wireless Grids used in locating the intruder.

![Wireless Grids](image)

**Figure 2.4 Wireless Grids [Achi 2008]**

RF fingerprinting performs better compared to other technique discussed. The first disadvantage is that the RF technique is that it cannot identify the hacker or attacker who
performs illegal activity from outside the building. The second disadvantage is that the RF custom installation requires a lot of manual setup and a lot of time. The third disadvantage is that once the RF fingerprinting has been set up, any modifications or changes in the environment, requires calculation of the entire RSSI (Received Signal Strength Indication) and the entire database has to be changed [Achin2008].

In wireless grid architecture of RF fingerprinting, the access points are placed in a structured format. The other approaches in RF fingerprinting places the access points in sparse locations. In RF fingerprinting, an initial setup configuration is needed. Whenever new equipment is added to the system it again requires setup configuration to take place. Instead of moving around the entire network and taking the RSSI values from different locations. The wireless grid offers a simple solution. In structured grid, mark on a map the location of access points within the office. A circle is drawn around the access point indicating the signal strength. The smaller the circle, the greater is the signal strength. Wireless Grid architecture has several disadvantages. The wireless grid architecture is only used to determine the device within a single floor of a building. When the device is placed on other floor of the same building, the wireless grid architecture does not provide the distinction. Not only the wireless grid architecture, but also the RF fingerprinting also cannot provide an effective solution. So much research has to be still focused on intrusion detection techniques in determining the hacker or intruder.

2.3. Sources of evidence from Wi-Fi

The Wireless access points and Wireless router integration are the sources of evidence in wireless network.

1) Wireless Access Points

This method helps to find useful information like who accessed a wireless network and from what location to computer investigators. For a successful investigation it is not only important to simply finding a wireless device or an access point, it is also important to determine the access points that are active in the network and devices connected to those access points.
For the reason of visibility of actual or attempts to connect, it is the responsibility of the forensic investigator to connect directly to a wireless access point via cable whenever it is possible. Using default access log-on responses the investigator must log-on to the network whenever it is connected to the access point. The investigator must resort to some other methods if the log-on attempts are unsuccessful and also if there is no cooperative information forthcoming [Turnbull 2008].

Having many different access points on wireless networks is one of the most important challenges that are encountered when monitoring and capturing wireless traffic. The problem will be raised when an investigator has the potential to examine only a portion of the channels, rather than having the capacity to examine all channels in a particular area. The issue of consolidating all of the files from different channels will be remained if the investigator is able to examine all channels in suspected area and also capture all traffic as well. The investigator can possibly reconstruct roaming sessions encounter using some of the freeware available to perform the task such as Wireshark if and only if the investigator has the ability to consolidate all of the files from different channels. If all the information is not captured, it is impossible to take a legally sound case [Turnbull 2008].

Time will be lost or at least fragmented, if there is any break in the transmission of the data when any signal is being transmitted. If the signal of the access point is weak, then the devices cannot be able to connect to the access point [Turnbull 2008].

Legal authority must examine the equipment on site and must be spelled out in search warrant before the investigator continues with the investigation. Computer forensic investigator can get a search warrant that can authorize the inspection of wireless components like laptops [Turnbull 2008].

However, computer investigator is not authorized to examine other devices like cell phones, PDA’s as they have ability to store information regarding to wireless network connections, thus it there is any on-site equipment that is not listed on the search warrant they must be taken off.
The forensic examiner has to be aware of the following things if they need for a live examination of wireless components.

- In the proximity of search warrant area there must be all active wireless access points
- In the area of search warrant there must be overlapping of all access points with signals
- The devices that have the ability to connect the access point with in the area or even the connected devices
- Wireless range capability of forensic examiner’s laptop NIC

A laptop computer must be maintained by a computer forensic investigator in which it has the wireless NIC such as the Proxim Orinoco 802.11b/g PCMCIA card that allows receiving wireless connections request to receive within the radius of the card. The wireless connectivity requests can cover a bigger range if the investigator can install NIC along with anti external antenna [Siles 2007].

There are also different types of software tools available like “airodump-ng” that provides a technique to find out which equipment is actively related with a wireless access point. To find relevant forensic tools “live-distribution CD” referred as “Back Track” is one of the most user-friendly downloadable applications [Siles 2007].

Equipment which attempt to access the wireless network must be pinpointed and at that time any attempt to connect wireless connection must be intercepted when the computer forensic investigator place laptop set to promiscuous mode. Packet tools like WinPcap and AirPcap are also useful for capturing the packets that are intercepted over a network [Siles 2007].

2) Wireless Router Interrogation

This method provides a detailed documentation on the IP addresses that have been leased in a given period, for example in a house if there is a wireless connection in which only two people live and each of them has their own laptops, then in the routing table there must be only two pieces of wireless components which have leased IP addresses. The forensic investigator
must start searching of the additional wireless components that may have illegal wireless components [Siles 2007].

To find out where the lease information is stored, the router must be interrogated. This type of interrogation can only be completed by the investigator to whom the laptop is directly connected to router for inspecting the table that contain routing information. Whenever a router is involved in the interrogation, time is the important factor to be considered because if the power is removed from the router, the information will be dumped by default in memory. The other important reason for the time factor is that IP leases have a life period so that it could be anywhere from 24 hours to particular number of days. There will be always IP address that a user access an external network and that IP address can provide trace- back information to the user [Siles 2007].

The investigator has to face some challenges if the suspect has changed the default security key of the router. The investigator must attempt different trials by using different log on keys like using the user-name “ blank” and password as “admin” and also investigator may also use username as “admin” and password as” password”. [Siles 2007].

2.4. Using Wireless Forensics tools

A variety of tools are now available to the network administrators to perform the remote shutdowns, monitor device use. Freeware tools those are available in both the UNIX and Windows environments are discussed. This list of tools for examining the windows products are Sysinternals (www.microsoft.com/technet/sysinternals/). The following are some of the important Sysinternals tools available.

RegMon – shows all the registry data in real time

Process Explorer – At a specific time what are all the loaded in the files, registry keys and dynamic link libraries (DLL).

Handle – list all the files and processes that are using those files.

Filemon – shows the entire file system activity.
There are certain tools that are available to monitor the network effectively. These are the PSTools (suite created by the Sysinternals).

PSEexec – runs processes remotely.

PsGetSid – this displays the service set identifier of the system or the user.

PsKill – this kills the process by name or processed.

PsList – this lists all the information about the processes.

PsLoggedOn – which user is locally logged into the system.

PsPasswd – allows for changing the account passwords.

PsService – the investigator gets the access to view and also control the services.

PsShutdown – allows the remote system to shutdown and optionally restart.

PsSuspend – allows for the suspension of the processes.

These tools are extremely useful to the network investigators. But if the hacker gets access to these tools then the damage is severe [Carrier 2010].

There are also several Linux/UNIX tools which are available which help the forensics investigators. Knoppix Security Tools Distribution is a bootable Linux CD which helps the forensics investigators. In the first case adjust the BIOS settings of the system such that the computer boots from the Knoppix CD. The Knoppix contains some forensically sound tools that are put together by Klaus Knopper (www.knoppix.net). These tools are now maintained by the Knoppix users. Knoppix offers a variety of tools in different categories that include the authentication, encryption, forensics, firewalls, IDS, honey pots, network utilities, packet sniffers, vulnerability assessment, and wireless tools. Some of the important Knoppix tools include the following [Carrier 2010].

Dcfldd – this is the U.S. DOD computer forensics lab version of the dd command.

Memfetch – this forces a memory dump.

Photorec – this tries to retrieve the image files from a digital camera.

Snort – this is used to perform the packet capture and analysis in the real time.

Oinkmaster – this tries to manage the snort rules, so as to decide which items must be ignored as regular traffic and which to be as irregular and raise alarms.

John – this is the latest version of password cracker.
chntpw – this enables to reset the password on a windows computer including the password on an administrative account.

Tcpdump – packet sniffer.

Ethereal – packet sniffer.

Another Linux tools is The Auditor (www.remote-exploit.org/?page=auditor). This forensics tool has a Trojan horse as its logo. This Auditor tools is based on Knoppix and has more than 300 network tools in it. These tools are used for network scanning, brute-force attack, bluetooth and wireless network. This Auditor is easy to implement and is updated easily. This comes along with other forensics tools such as Autopsy and Sleuth Kit. This also performs password cracking as it contains the word listing from many languages. This also includes the built-in web browsers, editors and graphic tools so that they can be used to generate reports.

Packet sniffers are the devices/software placed in the network, which is used to monitor the traffic. For increasing the security and tracking the bottlenecks in network packet sniffers are used. But attackers use them illegally to obtain the network traffic information. In TCP/IP networks packet sniffers examine the packets and hence they are given that name. Windows has many sniffing tools available, but they cannot feed the directly collected data to the other tools. Programs such as Tcpdump, Ethereal and Snort can read the data collected in Pcap format. Pcap is called Libpcap in Unix/Windows and is called Winpcap in Windows. If the network is being hit with the SYN flood attacks, the forensic tool must be able to determine the packets with SYN flag set. To be able to determine these packets Tcpdump, ethereal, and snort are programmed to determine the TCP headers [Meghanathan 2009]. Figure 2.5, Figure 2.6 and Figure 2.7 shows the IP header format, TCP header format and UDP header format respectively.

| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| **Version** | **IHL** | **Differentiated Services** | **Total length** |
| **Identification** | **Flags** | **Fragment offset** |
| **TTL** | **Protocol** | **Header checksum** |

**Source IP address**

**Destination IP address**

**Options and padding ::**

![Figure 2.5 IP Header Format](image-url) [Meghanathan 2009]
Tcpslice (http://sourceforge.net/projects/tcpslice/) is a good forensics tool that is used for the extraction of the information from large Libcap files. Just in this tool, the investigator has to mention the time-frame at which the information has to be extracted. A suite of tools (http://tcpreplay.synfin.net/trac) is used to replay the traffic recorded in the Libpcap format. This is used to test the network devices such as the IDS, switches and routers. Tcpdstat (www.freesdsoftware.org/net/tcpdstat.html) is another forensic tool which gives a quick review on the network traffic in the real time. This forensic tool generates the Libpcap statistics and
breaks down the packets by protocol. This tool also gives information regarding the average and maximum transfer rates [Carrier 2010].

Ngrep (http://ngrep.sourceforge.net) is used to examine the e-mail headers and IRC charts in the network traffic. This forensics tool is similar to TCPdump, but this is also used to identify the communication between the worms and viruses. Etherape (www.etherape://sourceforge.net/) is another tool that is used to view the network traffic graphically. Ethereal comes with Knoppix STD and the Auditor offers the Windows version of Ethereal. Ethereal can be used in the real time environment to open the traced files from the packet captures. The important feature of it is to rebuild the sessions. The modified version of Ethereal is the Wireshark (www.Wireshark.org).

Netdude (http://netdude.sourceforge.net) is used to analyze the large TCPdump files with an easy-to-use interface. Argus (www.qusient.com/argus) is an analysis, session data probe and a collector tool [Carrier 2010].

Ettercap is a terminal based network sniffer/logger and interceptor. It is majorly used for Ethernet LAN. Active, passive dissection on many protocols is possible in Ettercap. Data injection and filtering is also possible in Ettercap. It also supports the use of plugins. It supports many sniffing modes so as to give a powerful and complete sniffing suite. It uses OS fingerprints to check the geometry of LAN. It has also ability to check whether a particular system is in a switched network or not [Lyon 2007].

Dsniff is a set of powerful network penetrating and auditing tools. It contains a suite of powerful network auditing and penetration-testing tools. It includes many tools such as dsniff, filesnarf, webspy and more. It monitors the network for some interesting data. It tries to implement the active man-in-the-middle attacks against the ssh and http sessions, here it tries to exploit the weak bindings in the ad hoc PKI. Dsniff is a powerful tool that handles the entire password sniffing [Lyon 2007].

Kismac is a passive GUI wireless stumbler. This is extremely used in MAC OSX. Like
Kismet, Kismac offers a nice GUI. This also in addition does the decryption and de-authentication attacks. It also offers the mapping in Pcap import and logging. The coding of Kismac is entirely different from Kismet, although the functionality of both of them is the same. Ntop is a network traffic usage monitor. This displays the network usage in a standard GUI. This is similar to what the top does for the processes. In the interactive mode it displays the network status at the user’s terminal. It acts as a Web server in the Web mode. The network status is stored in the HTML dump. It uses RRD for storing the network statistics. It also does Ntop-centric monitoring applications by using the HTTP-based client interface [Lyon 2007].

The SolarisWinds contains a large number of discovery/monitoring attack tools. This organization creates and sells many special tools for the system administrators. It contains several security related tools. It contains network discovery scanners, SNMP brute-force cracker, TCP connection reset program and router password decryption program. In addition to these it contains the fastest router config download/upload applications [Lyon 2007].

Nagios is an open source network monitoring program. It keeps a watch on the services and hosts that are specified. It tries to alter when the things go worse or when it gets better. The major work of this tool includes the monitoring of the network services. The services include the SNMP, POP3, HTTP, PING and more. It also enables the monitoring of the host services such as the processor, load, disk usage and more. It also sends the notifications when the service or the host problems have occurred. This is done through the email, pager or other user-defined method [Lyon 2007].

The Honeynet (www.honeynet.org) was developed with a single motive for information availability stop the network and internet attackers. There are many people who participate in this worldwide project. The objective of this project is information, tools and awareness. The first objective is to make the people and organizations that threats exist and seconds is to provide the information regarding how to protect from these threats. Honeynet offers a variety of tools and methods to protect from these attacks. The recent major threat is the distributed denial-of-service attack. This attack doesn’t go no only goes through the organization local ISP, but also through other organization network. In DDOS hundreds or even thousands of machines are used. These machines are called zombies. The major concern with these attacks is time taken to detect
these attacks and also high monetary impact. Another major attack is the zero day attacks. The attacker just tries to see the loop holes present in OS. The vendor usually does not have any idea of these attacks. So the vendor haven’t released patches to these loop holes. The Honetnet project helps the administrators as a resource to protect from attacks such as Distributed Denial of Service attacks and other attacks. The honeypot looks like any other computer in the network. Its purpose is to lure the attackers. This doesn’t contain any information of real value. When there is an attack on the honeypot it is taken offline and the remaining systems on the networks run as it is. Honeywalls are setup to monitor what is happening in the honeypots and record the activities of the attacker [Carrier 2010].

CurrPorts is a network monitoring software which displays all the TCP/IP/UDP ports that are open on the computer. For each port that is opened, a detailed explanation of process that opened that port is known. The detailed information includes the process that opened the port, name of the process, the full path of the process and version information of the process, the time of creation of the process and the user who created it. The CurrPorts also closes the process that has opened the TCP connection, unwanted TCP connection, save the TCP/UDP ports information in an HTML file. When the TCP/UDP ports are owned by unidentified applications, CurrPorts automatically marks them pink [Sofer 2001]. Figure 2.8 shows CurrPorts network monitoring software displaying TCP/IP/UDP ports that are open on a computer.

![Figure 2.8 CurrPorts](image-url)
Smartsniff is a network monitoring utility which captures all the TCP/UDP packets in the network. It also shows all the data that has been captured. It shows the captured data as the conversations between the clients and the server take place. The TCP/IP conversations can be viewed in ASCII mode in the case of text based protocols. They are the HTTP, SMTP, POP3 and FTP. In the case of non-text based protocols they can be viewed as hex dump.

This utility provides three ways of capturing TCP/IP packets [Sofer 2001]

1) The data is captured as raw sockets. This allows the capturing of the data without the need for a capture driver. It has some severe limitations.

2) In the second case WinPcap capture drivers are installed. This allows for the capture of the data on all the Windows operating systems. WinPcap is an open-source capture driver that is available. This is the preferred way to capture TCP/IP packets and shows better performance compared to the raw sockets.

3) Microsoft Network Monitor Driver is now recently used in Windows 2000/XP. This can be used by SmartSniff. This driver is not default installed, but has to be manually installed. This can be installed from CD-ROM of Windows 2000/XP or from Windows XP Service Pack2 Support Tools. This has a tool called netcap.exe. If this tool is run for the first time this driver gets installed. For Windows 7/Vista Microsoft Network Monitor driver three is used by the SmartSniff to capture the network traffic. New version Microsoft Network Monitor driver 3.X is now available in the Microsoft website.

Figure 2.9 shows SmartSniff capturing window. Figure 2.10 shows various capturing options in SmartSniff. Figure 2.11 shows capturing with WinPcap capture drivers.
Figure 2.9 SmartSniff capturing window.

Figure 2.10 Capturing options in SmartSniff.
The Adapter Watch displays the information regarding the network adapters. It displays the IP addresses, DNS servers, WINS servers, MTU values and the number of bytes sent or received. It also displays the statistics regarding the TCP/IP/UDP/ICMP protocols of the local computer [Sofer 2001]. Figure 2.12 shows Adapter Watch displaying information about network adapters.
PingInfoView allows pinging the multiple hosts and IP addresses and putting them together in a single table. It allows pinging the hosts every number of seconds that the administrator specifies and displays the results in a single table. It displays both the succeed pings, failed pings and the average ping time [Sofer 2001]. Figure 2.13 shows PingInfoView that pings multiple hosts and IP addresses.

![Figure 2.13 PingInfoView](image)

FastResolver tries to combine multiple host names into IP addresses and vice versa. If the list of IP addresses is specified, then FastResolver scans only in the range that has been given. Fast resolver also gives the information regarding the MAC addresses of the hosts that has been given [Sofer 2001]. Figure 2.14 shows FastResolver combining multiple host names and IP addresses.

![Figure 2.14 FastResolver](image)
WirelessNetView monitors the activities in networks that are around the local network. It acts in a similar way as that of a Netstumbler. For each network that has been detected, SSID, the average signal quality, the authentication algorithm that is used, MAC address and more are displayed [Sofer 2001]. Figure 2.15 shows WirelessnetView monitoring activities in networks that are around the local network.

![WirelessNetView](image)

**Figure 2.15 WirelessnetView**

NetRouteView displays the routes on the current network. It is similar to Route.exe. It displays the destination, interface IP addresses, mask, gateway, protocol, MAC address and the interface name. This Netrouteview allows for the removal of the existing static routes and also adding up of the new routes [Sofer 2001]. Figure 2.16 shows NetRouteView that displays routes on the current network.
### Figure 2.16 NetRouteView

<table>
<thead>
<tr>
<th>Destination</th>
<th>Mask</th>
<th>Gateway</th>
<th>Interface IP</th>
<th>Metric</th>
<th>Type</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>192.168.10.1</td>
<td>192.168.10.33</td>
<td>30</td>
<td>Indirect</td>
<td>Static Ro</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>255.0.0.0</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>306</td>
<td>Direct</td>
<td>Static Ro</td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>255.255.255.255</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>306</td>
<td>Direct</td>
<td>Static Ro</td>
</tr>
<tr>
<td>127.255.255..</td>
<td>255.255.255.255</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>306</td>
<td>Direct</td>
<td>Static Ro</td>
</tr>
<tr>
<td>192.168.10.0</td>
<td>255.255.255.0</td>
<td>192.168.10.33</td>
<td>192.168.10.33</td>
<td>286</td>
<td>Direct</td>
<td>Static Ro</td>
</tr>
<tr>
<td>192.168.10.33</td>
<td>255.255.255.255</td>
<td>192.168.10.33</td>
<td>192.168.10.33</td>
<td>286</td>
<td>Direct</td>
<td>Static Ro</td>
</tr>
<tr>
<td>192.168.10.255</td>
<td>255.255.255.255</td>
<td>192.168.10.33</td>
<td>192.168.10.33</td>
<td>286</td>
<td>Direct</td>
<td>Static Ro</td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>306</td>
<td>Direct</td>
<td>Static Ro</td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>192.168.10.33</td>
<td>192.168.10.33</td>
<td>286</td>
<td>Direct</td>
<td>Static Ro</td>
</tr>
<tr>
<td>255.255.255..</td>
<td>255.255.255.255</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>306</td>
<td>Direct</td>
<td>Static Ro</td>
</tr>
<tr>
<td>255.255.255..</td>
<td>255.255.255.255</td>
<td>192.168.10.33</td>
<td>192.168.10.33</td>
<td>286</td>
<td>Direct</td>
<td>Static Ro</td>
</tr>
</tbody>
</table>
3. PROPOSED SYSTEM DESIGN

Wireshark is based on Winpcap library. It needs Winpcap drivers to be installed and the network card must be compatible with it. This project mainly focuses on implementing PacketXtract tool (X platform) that is similar to Wireshark and uses the socket programming. Here X in ‘PacketXtract’ means that this tool is cross-platform and can run on any hardware out of box. The main advantage of using sockets is that they have core network functionality and can run on any hardware out of the box. First program creates the raw socket. The socket is then bound to the local IP.

There are two parts in the design of the implemented program. They are the GUI and Listener. GUI is divided in three parts. They are the menu, packet list and packet details. GUI is in the Main Window class.

The menu contains the following options. They are described below.
- Start : begins packet listening
- Stop : stops packet listening
- Option: choose interface to listen to
- Analyze: starts analyzing TCP packets to find

The packet list lists the packets that were captured. They are listed in order of time that they were captured. Other information regarding packet source, packet destination, and packet protocol is also obtained.

The Packet details show the detailed information about the selected packet. IP, TCP and UDP headers of the packet transmitted is also described. Figure 3.1 shows the QTcreator opening the implemented program. Figure 3.2 shows the GUI containing Start, Stop, Options and Analyze. It also displays the packet list and packet details. When the options in GUI is clicked the interface GUI is displayed. Figure 3.3 shows the GUI interface. It displays the interface on which implemented packet sniffer is run. Injected packets are often TCP segments with the FIN or RST flags set. Figure 3.4 shows the analysis of the suspected injected packets.
Figure 3.1 QtCreator to open the implemented design

Figure 3.2 GUI Menu List
The implemented program does packet listening and injection into the network. In order to enable Packet listening, program calls WSAIoctl() on the socket with SIO_RCVALL option.
Next there is an infinite loop that calls recvfrom and feed the buffer. Recvfrom is a function that actually reads data from the socket. Injected packets are often TCP segments with the FIN or RST flags set (also known as “FIN packets” and “RST packets”). Each of these flags indicates that a computer does not want to continue a TCP conversation. So, when there is a high amount of this kind of packets there is good probability that the sender is injecting packets.

Listener runs in different thread. This thread is started in Mainwindow constructor.

1) Listening is initialized in the Listener::run () function
- initialize the winsock library:
  
  
  WSAStartup(MAKEWORD(2,2), &wsa)

- Create Raw Sockets
  
  Sniffer = socket (AF_INET, SOCK_RAW, IPPROTO_IP)

- Retrieve the available ips (interfaces) of the local host
  
  Local = gethostbyname (hostname);

2) Listening is started in Listener::Start () function (Start function is called when user click on Start menu):
- binding the socket to the chosen ip and port 0
  
  Memset (&dest, 0, sizeof(dest));
  
  memcpy(&dest.sin_addr.s_addr,local->h_addr_list[in],sizeof(dest.sin_addr.s_addr));
  
  dest.sin_family = AF_INET;
  
  dest.sin_port = 0;
  
  bind (sniffer,(struct sockaddr *)&dest,sizeof(dest))

  The AF_INET is the address family for IPv4 so the socket listens to all packets.

3) Next the socket is set to listen for the packets

  WSAIoctl(sniffer,SIO_RCVALL, &j, sizeof(j), 0, 0, (DWORD*)&in,0, 0)

  SIO_RCVALL is the parameter that makes socket actually listens to packets.

4) After setting the socket then listen to the packets. It's being done in Listener::Start Sniffing function.

The main part in the program can be described with the following code.

```
While (mangobyte > 0){
  mangobyte = recvfrom(sniffer,(char*)Buffer,65536,0,0,0) ;
  ProcessPacket (Buffer, mangobyte,packet);
```
So in a loop packets are read by recvfrom function to a buffer. And then they are processed by ProcessPacket function. ProcessPacket reads type of a packet and calls appropriate function. For example if packet is TCP packet it calls PrintTcpPacket function. These are the family of the functions that interprets the packets.

```c
void ProcessPacket (unsigned char*, int, Pakiet& packet);    //This will decide how to process the packets
void PrintIpHeader (unsigned char*, int, Pakiet& packet);    //print the IP header of packet
void PrintIcmpPacket (unsigned char*, int, Pakiet& packet);    //print the ICMP header of packet
void PrintUdpPacket (unsigned char*, int, Pakiet& packet);    //print the UDP header of packet
void PrintTcpPacket (unsigned char*, int, Pakiet& packet);    //print the TCP header of packet
void PrintData       (unsigned char*, int, Pakiet& packet);    //print the raw data
```

All the packets are described as structures in a listener.h file. They are the ip_hdr, udp_hdr, tcp_header, icmp_hdr. All packets are stored in a memory in QList<Packet> structure named "packets. It is possible to analyze every packet that was captured. Also it is used by Mainwindow to display the info on the GUI. Here, a detailed test case of the implemented project is also presented in the Evaluation.

4. EVALUATION AND RESULTS

Wireless AP isn’t always as secured as they should be. Wi-Fi is now majorly used in public unsecured networks. Public Wi-Fi tends to be most unsecured network. Here, test cases on different types of attacks and its forensic analysis are presented. These test cases on different types of attacks are not related to the wireless packet sniffing tool. This is only just used as a additional reference that helps in understanding the attack scenarios in real-time. The test cases on different packet sniffers used to listen and analyze the traffic is also presented.

MAC ADDRESSES SPOOFING:
The tools that are used in Mac address spoofing include the Linux distro tools like Ubuntu, Backtrack3 or Backtrack4 with airodump-ng and macchanger. Here, the demonstration on MAC address spoofing on a public unsecured network is presented.

**Step 1:**
Find your target. In this case it will be access point in the public unsecured network.

**Step 2:**
Connect to the Wi-Fi access point to see if it’s working. Figure 4.1 shows the attacker connected to wireless access point.

![Figure 4.1 Connected to the wireless access points](image)

**Step 3:**
See whether there is access to the internet in public unsecured network. Figure 4.2 shows the attacker checking access to the internet.
Some public unsecured networks won’t let the access to the internet. If the person has a valid registration then the person is allowed to access the internet. So, to gain access to such public networks, MAC address spoofing is used.

**Step 4:**

To be able to spoof MAC address, MAC address that has to be spoofed must be known. To find the MAC address Wi-Fi card has to be put in monitor mode. If Wi-Fi is used through USB, interface is rausb0. If Wi-Fi is not connected through the USB, then the interface used is wlan(). Figure 4.3 shows Wi-Fi connected through USB.
Step 5:

The Wi-Fi is in monitor mode. The tool airodump-ng is used to find out the MAC address. This MAC address is used for spoofing to gain free access to the internet. Figure 4.4 shows airodump-ng finding out the MAC address to spoof. Figure 4.5 shows the obtained spoofed MAC address through airodump-ng tool.
Figure 4.4 Finding out the MAC address to spoof

Figure 4.5 Obtaining spoofed MAC address
BSSID of public unsecured network is highlighted because this step helps in finding the MAC address to spoof. One can fake as authorized user that are paid and is therefore connected to public unsecured network.

**Step 6:**

In this step, authorized user registered to the network can be found out. This can be done by examining the packet count. Figure 4.6 shows the attacker finding out the unauthorized user on the network.

![Airodump-ng sniffs the public unsecured network to listen to packets.](image)

**Figure 4.6** Finding authorized user connected to the network

Airodump-ng sniffs the public unsecured network to listen to packets.
The highlighted part in Figure 4.7 shows the MAC address (00:22: FA: 47:93:86) that has the most packets sent and received by being connected to the public unsecured network. The highlighted part is from where there is a maximum packet that is getting transmitted. So, this MAC address is being used to gain free access to the internet.

**Figure 4.7** Finding the MAC address to spoof

Step 7:

Spoof the MAC address by using tool macchanger. Before using this tool Wi-Fi card has to be removed from monitor mode. This can be done using the command `ifconfig rausb0 down`. Figure 4.8 shows the attacker spoofing current MAC to the faked MAC.
Figure 4.8 Spoofing the current MAC to Faked MAC

After changing the original MAC address to spoofed one, Wi-Fi card has to be brought down to the normal mode. Figure 4.9 shows the successful spoofing of the MAC address by the attacker.

Figure 4.9 Successful MAC address spoofing.
The MAC address has been changed successfully and the Wi-Fi card has been brought down to normal mode. Figure 4.10 shows Wi-Fi brought down to normal mode after the attack has been completed.

Figure 4.10 Wi-Fi brought down to normal mode.

**Step 8:**

After the MAC address has been spoofed, just try to connect to the public unsecured network.

Figure 4.11 shows attacker connecting to the public unsecured network after faked MAC. Figure 4.12 shows attacker checking access to internet in public unsecured network. Figure 4.13 shows the attacker gaining access to the internet in public unsecured network using faked MAC address.

![Figure 4.11](image)

**Figure 4.11** Connecting to the public unsecured network.
Figure 4.12 Checking the access to internet in public unsecured network

Figure 4.13 Attacker gaining access to internet
The public unsecured network believes that the person is an authorized user that paid for internet access and can surf internet for free.

**Wireshark**

The next test case is on Wireshark. Wi-Fi sniffing is used in a forensics investigation. Wireshark is a popular network sniffer for both windows and Linux. It can sniff Wi-Fi packets and wired packets. Unfortunately it doesn't have much use to sniff traffic unless it’s all happening on the same network. To start wireshark sniffing choose the Wi-Fi card in Wireshark, it is usually set to default.

Click the start capture button in the Wireshark and it is presented with the following screen as shown in Figure 4.14.

![Figure 4.14 Packet capturing in Wireshark](image)

Figure 4.14 gives many details like what is the IP address of computer that is sending the request (Source), and what is the receivers IP address (Destination). It also displays the type of protocol being used for packets transfer and information about more complex details of how sent and received packets are being treated. There is also information regarding TCP or UDP packet and how it is being crafted. Figure 4.15 shows the data that is being transmitted. In case of http
one can read the data, but to filter http data there is option in analyze menu as shown in Figure 4.15.

![Figure 4.15 Http filtering in Wireshark](image)

The display filters in Wireshark is shown in Figure 4.16.

![Figure 4.16 Display filters in Wireshark](image)
In Wireshark there are different options for filters. Filters can be applied to TCP data, UDP data or http. In Figure 4.17 http is selected as a filter in Wireshark.

As it is shown data transmitted between 192.168.1.3 and 109.72.91.48 can be known. Very useful at public places and if someone isn't using https when entering login and password details, well it's self explanatory what can be done.

**WEP key cracking**

Today almost everything in computer industry has a password to avoid someone stealing important data or deleting it and accessing files and folders that are supposed to be secret. That is also the case when it comes to avoiding someone accessing wireless access point without being authorized to do so. Here, WEP key cracking attack on wireless access points is discussed. WEP key is weak encryption protocol by today’s standards and is easier to crack by gathering many
packets that are being transmitted over the Wi-Fi network and trying to determine from the transmitted packets what the password/key may be. For determining password/key, tools like airmon-ng, airodump-ng, aireplay-ng and aircrack-ng are used.

The tool airodump-ng is used for wireless forensic analysis of transmitted packets. It gives the information regarding transmitted packets and also about senders and receivers information. Tools aireplay-ng and aircrack-ng are used to capture important data that's being transmitted over the Wi-Fi and to crack it using airocrack.

**Step 1** - is setting the Wi-Fi card into monitor mode and for this airmon-ng is used. For starting the Wi-Fi #airmon-ng start rausb0 is used. Figure 4.18 shows Wi-Fi in monitor mode.

```
sudo airodump-ng -c 6 -w wep -i ath1
```

- `c` = channel which target network is transmitting on
- `w` = Dump file prefix
- `i` = Save only captured IVs
- `ath1` = wireless interface name

![Figure 4.18 Wi-Fi in monitor mode](image)

**Step 2**
Figure 4.19 Initial output

Figure 4.19 shows an initial output screen when airodump-ng gets started. Here 00:17:9A:9F:05:51 is the wireless access point that the hacker wants to attack.

**Step 3**

In this step testing whether injection of packets is working is done, here ath1 instead of rausb0 because the Wi-Fi card isn't USB connected. This is done in new terminal tab or new terminal without closing the previous one. Figure 4.20 shows testing of injection of the packets in aireplay-ng. Figure 4.21 shows successful packet injection in aireplay-ng.

Figure 4.20 Testing injections of packets
Figure 4.21 Successful working of packet injection

Step 4

Start with gathering of important packets/data for cracking the key. Send arp request to speed up the process is used. Figure 4.22 shows gathering packets for packet injection in aireplay-ng.

Figure 4.22 Gathering packets/data for cracking key

-3 = standard arp request replay
-b = access point MAC address
-h = source MAC address (either an associated client or from fake authentication)

Figure 4.23 Capturing ARP requests
Figure 4.23 shows capturing of ARP requests has started and it’s being saved for later analysis in replay_arp-0510-113257.cap

**Step 5**

Start the cracker, aircrack-ng. Start it in new terminal tab or new terminal. Don't close previous terminal windows or tabs. Figure 4.24 shows Aircrack initialization. Figure 4.25 shows the Aircrack process and Figure 4.26 shows cracked password key using aircrack-ng.

```
ubuntu@openwrt:~$ sudo aircrack-ng -a 1 -o -n 128 wep-01.ivs
Password:
```

- `-a = Force attack mode`
- `1 = static WEP`
- `-0 = Apply colors in Aircrack`
- `-n = Specify the length of the key (128 for 104-bit WEP)`

**Figure 4.24** Aircrack initialization
Figure 4.25 Aircrack process

Figure 4.26 Cracked password key
Wi-Fi sniffing

Wi-Fi sniffing means to use various wireless forensics tools and to try to see what is happening on various Wi-Fi access points. Things like who is connected to certain wireless access point and what are they doing can be seen by sniffing the traffic over wireless network. Depending on wireless access point one can sometimes see readable text indicating that the wireless access point is unencrypted and user that is connected to it is using http to access some websites as opposed to https. To be able to sniff wireless network the forensics investigators need to have certain tools to do it. The best tool for this job is kismet. Kismet is a wireless packet sniffer, and it can also be used to determine how strong the signal of certain wireless access point is. Apart from kismet and airmon-ng it doesn't need anything else, everything else comes with Linux by default.

Step 1

When using kismet, airmon-ng for Wi-Fi sniffing the Wi-Fi card is set in to monitor mode. After doing that, a public place where many people use Wi-Fi connection is found. The more the connections the better it is. For starting Airmon-ng command #airmon-ng start wlan0 is used.

Step 2

Type in Kismet and press enter to start the kismet. Figure 4.27 and Figure 4.28 shows running kismet.

```
root@bt:# kismet
```

Figure 4.27 Running Kismet
Figure 4.28 Running Kismet (contd...)

Figure 4.29 Running Kismet as root
In Figure 4.29 there is warning because kismet runs as a root. It doesn't present that much of a danger and it’s easier to run it as root. If the user is new to the command, the user can use command sudo kismet. In figure 4.29 the user is asked to start Kismet server, just press yes. Figure 4.30 shows various startup options in kismet.

![Figure 4.30 Startup options in Kismet](image)

Logging option is to save all the captured data in a file. The Show Console is for the advanced stage and it is used for sniffing.

**Step 3**

Just press ‘Yes’ to start capturing of data. The wireless card must be set to be wlan0 or rausb0. Here wlan() is used in this example. Figure 4.31 shows adding the interface to the wireless card.
Figure 4.31 Adding interface to wireless card.

Pressing ‘Yes’ will present with place where to enter your wireless card name (wlan0 in the example). Figure 4.32 shows three fields, the first one is marked. Intf is the important one and the other two can be ignored.
Figure 4.32 Entering wireless card name in kismet

Figure 4.33 BSSID/MAC address
Figure 4.33 shows name for each wireless access points. Highlighting any of the wireless access points will present with the BSSID/MAC address. Pkts is showing how much data/packets are being transmitted over each wireless access points. If there are a lot of packets being transmitted, then it means that someone is being very active while connected to that wireless access point with their computer and it means good chances for seeing what data they are transmitting via http, if they are using http. Figure 4.34 shows Client list in kismet. The client list contains MAC address of users that are connected to the particular wireless access point. Client List isn't set by default, to set it go to View and click on Client list.

Figure 4.34 Client list

Various other options of what the investigator want to see and what wants to be hidden can also be set.

Step 4

To see what is in the captured data, open console and enter mc.
Just find the folder where the kismet is started. In this case, it is the default folder root.

The investigator tries to find out the file that starts with kismet and ends with .pcdump as shown in the Figure 4.37.
Figure 4.37 Finding file starting with kismet and ending with .pcdump

If key F3 is pressed Figure 4.38 is presented.

Figure 4.38 Pressing key F3
It recognizes names of some of the wireless access points like 2WIRE969 and QWERTY. Click on Search in the bottom of the screen or press F7 to do a search. Enter search string like .com or host like .com. Figure 4.39 shows searching string .com.

![Figure 4.39 Searching string like .com](image)

Continue repeating this process of search until a meaningful screenshot is obtained with much information.

![Figure 4.40 Repeated searching](image)
The Figure 4.40 shows that a person in the network is using Twitter.

**DOS attacks on Wireless Access Points**

The term DOS stands for Denial of Service and it does just that, it denies service to users that are trying to access certain website or wireless access point. The tools Airmon-ng (it’s used to set Wi-Fi card in to monitor mode that is very important) and aireplay-ng (it is used for packet injection that is very important for this attack) mkd3 (the program that combines it all and does the DOS) are used in DOS attacks.

**Step 1**

Set Wi-Fi card into monitor mode and set channel to be the same number as the target's channel, like in this example. Figure 4.41 shows setting of the Wi-Fi in monitor mode.

![Figure 4.41 Setting Wi-Fi to monitor mode](https://example.com/figure441.png)
In the experiment DOS attack is chosen on 2WIRE484 access point. The MAC address of access point is 34: EF: 44:73:F9:A9 and channel is number 5. Figure 4.42 shows DOS attacks on channel 5 chosen on 2WIRE484 access point.

**Step 2**
Identify the target. Find target MAC address using wicd default Wi-Fi network manager

**Step 3**
Open a new text file and enter in it the target's MAC address. Save the file as target.txt and save it in the same directory with mdk3 which is in /pentest/wireless/mdk3.

**Step 4**
Go to the directory of mdk3, which is in backtrack4. The directory in this experimentation is /pentest/wireless/mdk3.

**Step 5**
Start first DOS attack, it is called de-authentication attack. Figure 4.43 shows starting DOS de-authentication attack.

**Step 6**
Start second DOS attack in new window, it is called Authentication DOS mode.
In Figure 4.44, Option -a means it is authentication attack. Option -m is Michael shutdown exploitation (TKIP) it cancels all traffic continuously. Option -i defines target's MAC address.

**Step 7**

Start third DOS de-authentication attack using tool aireplay-ng. It will continue flooding target MAC address and no one will be able to connect to it and those who were connected during attack will get disconnected. Figure 4.45 shows third DOS de-authentication attack using tool aireplay-ng.

**Figure 4.45** Third DOS de-authentication attack
Option -0 1000 defines size of packets to be sent. Option -a defines the target's MAC address. Option -h defines the attacker's MAC address.

**CommView**

This tool is used for listening and analyzing network packets. Main part of the program is the Captured packet listening, in addition it also displays the source and destination MAC and port. This tool can also be used for finding the possible packet injection. Figure 4.47 shows a statistics window that shows how many packet errors that were spotted. When there are too many errors the investigator can suspect that there is packet injection, then the tab Reports will show which packet is suspected. The suspected packet would have address of the attacker. Program has other functionality like listing network connections, vital statistics, protocol distribution charts. This tool is also capable of reconstructing TCP connections, viewing protocols distribution, bandwidth utilization, and network nodes charts and tables. Figure 4.46 shows listening to packets using CommView. Figure 4.47 shows analyzing packets using CommView.

![Figure 4.46 Listening to the packets](image-url)
Wireshark packet sniffing

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis and software and communications protocol development. It allows the user to see all traffic being passed over the network by putting the network interface into promiscuous mode. But it has much additional functionality, for example data display can be refined using a display filter. It can interpret and dissect many more protocols. Different kinds of packets are colored so it helps the forensics investigators to identify them. There is additional info column which has much important information. Wireshark has very complex analysis tool. This tool automatically show which packet are suspected, also suspected packets are colored red. Figure 4.48 shows listening to packets using Wireshark. Figure 4.49 shows analysis of captured packets using Wireshark.
Figure 4.48 Wireshark – Listening of the packets

Figure 4.49 Wireshark - Analysis
Tcpdump

Tcpdump provides the ability to analyze network behavior, performance and applications that generate or receive network traffic. It can also be used for analyzing the Network infrastructure itself by determining whether all necessary routing is occurring properly. This allows the user to further isolate the source of a problem. Main difference is that the GUI is in the text mode. Program only display the packet list. It displays only one packet per line. It is not showing the detailed packed information. Figure 4.50 shows listening to packets using TCPdump.

PLAB

This tool is very similar to the Tcpdump. It is also a text tool. Only difference is that it is the display of the packet contents. Figure 4.51 shows listening to packets using PLAB.
Network Miner

Network Miner can be used as a passive network sniffer/packet capturing tool as other tools. But it is more focused on collecting data (such as forensic evidence) about hosts on the network rather than to collect data regarding the traffic on the network. The packets are shown in the tree mode. This tool cannot analyze for the possible network intrusion. Figure 4.51 shows listening to packets using Network Miner.

Figure 4.51 PLAB – Listening to packets
Colasoft Capsa

This network analysis tool is very powerful and it has a lot more functionality. It is supporting more than 300 protocols. It can record global or scope-specific network Events, containing four types of log primarily generated by the advanced analyzers HTTP requests and email messages. It has view that visualizes all network connections and traffic details in one single graph. This program has a lot of functions. It displays packets in colored output. In the diagnostics tab there are messages that help in finding possible packet injections. Figure 4.54 shows Colasoft Capsa detecting ARP Scan. Figure 4.53 shows Colasoft Capsa listening to packets. Figure 4.54 shows analysis of captured packets using Colasoft Capsa.
Figure 4.53 Colasoft Capsa 8 – Listening to the Packets

Figure 4.54 Colasoft Capsa 8 – Analysis
PacketXtract Listening and Analysis

Wireshark is based on Winpcap library. It needs Winpcap drivers to be installed and the network card must be compatible with it. This project mainly focuses on implementing a program that is similar to Wireshark and uses the socket programming. The main advantage of using sockets is that they have core network functionality and can run on any hardware out of the box. When the implemented program is run on a QT Creator, it starts listening to the packets. Figure 4.55 and Figure 4.56 shows the implemented packet sniffer listening to the packets in the network.

![Packet Listener](image)

**Figure 4.55** Listening to packets on a network
Figure 4.56 Listening to packets (contd…)

Figure 4.56 shows GUI is divided into three parts. The first part is menu that contains the start, stop options and analyze. The second part is the ‘packet list’ that lists all the packets transmitting in the network. It lists the time (in milliseconds from the start of the capturing), Source and destination IP addresses and also the protocol used by these IP packets. The third part is the packet details. It lists all the details of the IP packet sent from the source to the destination. Just click on any of the rows in the GUI and detail listing of the packet is obtained. Figure 4.57 shows the packet details.
The entire structure of the TCP packet can be obtained in the packet list part of the GUI as shown below. The same is in the case of UDP, ICMP or any other packets.

**TCP Packet**

**IP Header**
- IP Version : 4
- IP Header Length : 5 DWORDS or 20 Bytes
- Type Of Service : 0
- IP Total Length : 52 Bytes (Size of Packet)
- Identification : 17680
- Reserved ZERO Field : 0
- Dont Fragment Field : 1
- More Fragment Field : 0
- TTL : 128

Figure 4.57 Packet details.
The second part in the menu of the GUI is the stop. If stop is clicked the listening to the packets in the network is stopped. The sniffing is stopped. When the options in the GUI menu are chosen, it manually asks the user to choose the interface. The investigator can manually choose any interface that has to be listened. Figure 4.58 shows packet sniffer stopping listening to the packets. Figure 4.59 shows choosing of interface by the administrator. The packet sniffer runs on the interface chosen.
Figure 4.58 Stopping the listening.

Figure 4.59 Choosing the interface
The next part of the implemented program is to find the injections in a network. Injected packets are often TCP segments with the FIN or RST flags set (also known as “FIN packets” and “RST packets”). Each of these flags indicates that a computer does not want to continue a TCP conversation. So, when there is a high amount of this kind of packets there is good probability that the sender is injecting packets. Figure 4.60 shows analysis of the captured packets.

Figure 4.60 Analysis of listened packets.
5. CONCLUSION

Wireless forensics is a relatively new field, but as computer intrusions become more common through this communication medium, new techniques, tools and laws are required to manage the acquisition and analysis of wireless data. In wireless networks, there are packet sniffing tools which are used to listen and analyze the traffic. The forensics investigator must choose the right tool that capable of listening and analyzing the network traffic. Wireshark is one of mostly used packet sniffer capable of analyzing and listening to the network traffic. It is based on Winpcap library. It needs the Winpcap drivers to be installed and the network card must be compatible with the Winpcap drivers.

In this project a detailed explanation on different wireless forensics tools available for Windows and Linux is presented. A detailed test case on generating and analysis of different attacks is presented. The attacks here include the MAC address spoofing, WEP key cracking, Wi-Fi sniffing and DoS attacks on wireless access points is presented. The detailed test cases on packet sniffers (Forensics tools) used to listen and analyze the traffic are presented. The packet sniffers that are discussed here are the Commview, Wireshark packet sniffer, and TCPdump, PLAB, Network Miner and Colasoft Capsa is presented. This project mainly focuses on implementing a packet sniffer that is similar to the Wireshark. It is similar in functionality to Wireshark, but it uses socket programming. The main advantage of using this socket is that they have core network functionality and can run on any hardware out of the box.
6. FUTURE WORK

Wireshark is one of mostly used packet sniffer capable of analyzing and listening to the network traffic. It is based on Winpcap library. It needs the Winpcap drivers to be installed and the network card must be compatible with the Winpcap drivers. This project mainly focuses on implementing a packet sniffer that is similar to the Wireshark. It is similar in functionality to Wireshark, but it uses socket programming. The main advantage of using this socket is that they have core network functionality and can run on any hardware out of the box. Wireshark implements many other functions such as capture filters, statistics about the packet flow between the source and destination. If these features are implemented in Wireshark, then it can be used in the real-world scenario. Still much of the work is yet remaining in implementing these features and designing a complete wireless packet sniffer with no compatibility issues.
7. BIBLIOGRAPHY


