WIRELESS LAN SECURITY ANALYSIS FOR IEEE 802.11 AND ITS TECHNICAL CHALLENGES, RECENT ADVANCES, AND FUTURE TRENDS

BY

IBBRAHIM

ID: 191-15-12148

JAYED BIN ISLAM

ID: 191-15-12434

MD. ABU RAYHAN ALIF

ID: 191-15-12069

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Gazi Zahirul Islam

Assistant Professor

Department of Computer Science and Engineering

Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

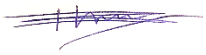
DHAKA, BANGLADESH

January 2022

APPROVAL

This research project titled "**Wireless Lan Security Analysis for IEEE 802.11 and its Technical Challenges, Recent Advances, and Future Trends**" submitted by **Ibbrahim**, ID No: **191-15-12148, Jayed Bin Islam,** ID No: **191-15-12434** and **Md. Abu Rayhan Alif,** ID No: **191-15-12069** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering (BSc) and approved as to its style and contents. The presentation has been held on January 2022.

BOARD OF EXAMINERS

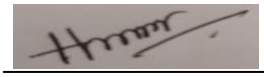


Chairman

Dr. Touhid Bhuiyan
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Moushumi Zaman Bonny
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Internal Examiner

Md. Mahfujur Rahman
Senior Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

External Examiner

Dr. Md Arshad Ali
Associate Professor
Department of Computer Science and Engineering
Hajee Mohammad Danesh Science and Technology University

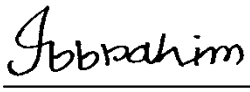
DECLARATION

We hereby declare that, the work presented in this thesis paper based on research project is done by us under the supervision of Mr. Gazi Zahirul Islam, Assistant Professor of Department of Computer Science and Engineering, Daffodil International University, in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering. We are declaring this report is my original work. We ensure that neither this report nor any part has been submitted elsewhere for the award of any degree.

Supervised by:

Gazi Zahirul Islam
Assistant Professor
Department of Computer Science and Engineering
Daffodil International University

Submitted by:



IBBRAHIM
ID: 191-15-12148
Department of Computer Science and Engineering
Daffodil International University

JAYED – BIN – ISLAM
ID: 191-15-12434
Department of Computer Science and Engineering
Daffodil International University

MD. ABU RAYHAN ALIF
ID: 191-15-12069
Department of Computer Science and Engineering
Daffodil International University

ACKNOWLEDGEMENT

Firstly, we can't show enough gratitude to the Almighty for showering His blessings and bestow us with a lot a patience and knowledge to make the Final year project happen successfully. If we can call the paper as successful one, it was all possible by the generosity of peers who lead us into the right direction. We would like to show our deep and sincere gratitude to the individuals who carried out tremendous support and expertise our work.

We would like to express our heartiest and cordial respect and gratitude to Gazi Zahirul Islam, Assistant professor, Daffodil International University, Department of Computer Science and Engineering. We are immensely influenced by Deep knowledge and keen interest of our supervisor that made our work to be a better manuscript to present. His enthusiastic nature, intellectual insights, tremendous guidance, constructive criticism, sharing his pearl of wisdom and reading many inferior drafts and correcting them at all stage have made it possible to complete the project.

We are truly beholden to the person who had not only supervised us also had the mantle of leadership throughout the whole journey of the project, He is none other than Professor Syed Akther Hossain, Head of The Department of Computer Science and Engineering, Daffodil International University, for his insightful guidance and also for providing resources we needed which lead us to right direction to complete the project.

Finally, we are truly grateful to our parents who always supported us and made us confident and strong enough to construct the project from scratch and also co-operated to complete the project.

ABSTRACT

Wifi, also known as WiFi or wifi, is a common technology that lets an electronic device wirelessly exchange data or connect to the internet. It does this by using radio waves to send and receive data. A lot of things make wifi good, like how easy it is to set up and how cheap it is. Furthermore, they don't bother you. At the same time, setting up a well-designed and safe wifi network is not easy. As a result, many businesses want help from experts to make sure that their wifi deployments or pilots are safe and don't hurt security or functionality. Security professionals can do wifi network surveys with a wide range of tools, from "free" open-source software to complex commercial software. Almost all of our businesses now use wireless networks to communicate, and security is one of the main concerns for us now. However, because open-source technologies aren't usually used for work, most businesses don't keep an eye on or check their networks. Professional and commercial auditing tools also cost too much for some businesses in our country. However, there are a lot of free tools that can help you find, monitor, and break into wifi networks, like Kismet, Wireshark, WiFiFoFum, Aircrack, and many more. This study aims to compare many security inspections that use different techniques, with the goal of finding out how difficult it is to use technology and how well the results are analyzed.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 01

INTRODUCTION

1.1 Introduction

It is possible to receive high-speed internet without the need for wires using wireless networking, sometimes known as Wi-Fi. Wi-Fi allows us to simultaneously connect numerous computers to the same high-speed internet connection. Within the wifi network's coverage area, anyone with a laptop or other wifi-enabled device can connect to the internet. There is no need for new phone lines or connections to be made with Wi-Fi [1].

A wireless network, including cell phones, televisions, and radios, uses radio waves. In reality, communication across a wireless network resembles two-way radio communication in many ways. Here's how it works:

i. Data is converted into a radio signal and delivered through an antenna by a computer's wireless adapter.

ii. The signal is received and decoded by a wireless router. The information is sent to the Internet via a physical, connected Ethernet connection.

In reverse, the router receives data from the Internet, converts it to a radio wave, and sends it to the computer's wireless adapter.

With numerous laptops and a wireless access point, setting up a Wi-Fi network is simple. A wireless network also necessitates the use of a router. This is a single unit that includes the following:

i. A cable or DSL modem connection port
ii. Router
iii. A network hub
iv. A security system
iv. A wireless access point

A wireless router is a device that allows us to connect computers and mobile devices to one another, as well as to a printer and the Internet, through the use of wireless or Ethernet signals. Despite the fact that walls and doors might interfere with the signal, most routers have a range of approximately 100 feet (30.5 meters) in all directions. Purchasing reasonably priced range extenders or repeaters to increase the range of the working router is necessary if the home or area where the network will be set up is large enough.

Many routers, like wireless adapters, can support several 802.11 standards. 802.11b routers are typically less expensive than other standards, however they are also slower than 802.11a, 802.11g, 802.11n, and 802.11ac routers due to the older standard. The most common routers are 802.11n routers. The router will begin working as soon as it is plugged in, and it will use its default settings. Most routers provide a Web interface that allows network administrators to adjust the router's internal settings.

As a result, the Administrator can choose from the following options:

i. The network's name, also known as the service set identifier (SSID), is: The manufacturer's name is usually the default setting.
ii. The router's channel is as follows: By default, most routers use channel 6. If the network builder lives in an apartment building and his neighbors use channel 6, he or she may face interference. Changing to a different channel should solve the issue.
iii. Optional security features on the router: Many routers use a standard, publicly accessible sign-on, so giving each user their own username and password is a smart idea.

To ensure the safety of a Wi-Fi network, both at home and in public, it is essential to keep it secure. Anyone with a wireless card can use a network administrator's signal if he configures his router to create an open hotspot. Most people, on the other hand, would like to keep outsiders out of their network. This necessitates a few security steps on the part of the network administrator.

The network administrator can also adjust other router settings to increase security. Additionally, the user can choose to block WAN requests, which prevent the router from responding to IP queries made by remote users, limit the number of devices that can connect to the router and disable remote administration. That's why you need to change the Service Set Identifier (SSID), or network name, so hackers can't tell which routers are connected to this network immediately away. Choosing a secure password is also a good idea. [2]

1.2 Motivation

- Today's people use wifi widely that's why its security question is not negligible.
- If we can't ensure data privacy then the whole internet system is worthless.
- In this domain many research has been done but there is not enough sophisticated result.
- In this research we want to prove that we can audit our network with some free software that will ensure our network safety.

1.3 Wi-Fi Security

But as Wi-Fi usage increases, so does the number of hackers. Security is the primary concern of those who use Wi-Fi hotspots. There is no way to secure these wireless networks. WeP and WPA aren't utilized to protect private wireless networks because of the difficulty of supporting users. You must also divulge the "private" encryption key when using WEP or WPA (s). Decoded Wi-Fi hotspot traffic does not require encryption because eavesdroppers already know one or more keys to do so.

Wi-Fi hotspots are routinely visited by hackers. When one free Wi-Fi hotspot is established, a bevy of new "free" Wi-Fi networks pop up, all offering to provide unrestricted access to the Internet. Wi-Fi hotspots that pretend to be legitimate but are actually fake are known as phishing sites. As soon as you check in, all of your private and confidential information is immediately gathered. These "free" networks put users at risk of being targeted by "channeling." Channeling is used by hackers and identity thieves to undertake man-in-the-middle attacks with the objective of gathering user names, passwords, and other sensitive data supplied by the user, and it is not a difficult process for the hacker.

A terrible idea is to tell the operating system to "remember" a given network (or SSID). False Wi-Fi networks, on the other hand, can set up their SSIDs such that they appear to be legitimate networks to the user's computer, allowing them to connect without their knowledge.

It is easy for hackers to obtain passwords by installing an unauthorized access point at an airport lounge. In many cases, Wi-Fi hotspot users are uninformed of the risks connected with using public wireless networks, and as a result, they do not take adequate safeguards to protect their personal information, privacy, or identity. Installers of hotspots deserve the same treatment. They may not be aware of the issues they face, or that they may assist protect user access by taking a few simple steps [3].

1.4 Attacking Way on Wi-Fi

Data Interception: Eavesdroppers can easily get their hands on data sent over Wi-Fi. They can get it within a few hundred feet with directional antennae, and even further with directional antennas. As a good thing, AES-CCMP data encryption and integrity are now supported by all Wi-Fi certified devices. The bad news is that some older devices only support TKIP, and many WLANs are set up to support both AES and TKIP. As for TKIP, its message integrity check (MIC) attacks allow a limited number of faked frames, like ARP, to be added. As long as the risks aren't too bad and the writing is on the wall, TKIP must be phased out in favor of AES-CCMP.

Denial of Service: WLANs are notoriously susceptible to denial-of-service (DoS) assaults. Because everyone uses the same unlicensed frequencies, competition is unavoidable in heavily populated areas. The good news is that when businesses migrate to 802.11n, they will get access to channels in the 5 GHz band that are larger and less congested, reducing "accidental DoS." Additionally, modern access points (APs) may change channels automatically to avoid interference. However, there are still considerations for DoS attacks: Phony messages are sent to disconnect users, consume AP resources, and maintain channel activity. Consider purchasing newer devices that include 802.11w management frame protection to protect against common DoS attack strategies such as Deauth Floods.

Rogue APs: Another major issue is the overloading of business networks by unknown, illegal APs. Fortunately, most business WLANs now employ genuine APs to scan channels in their leisure time for potential rogues. Unfortunately, identifying the wired network connectivity of "real rogues" is a talent that conventional WLAN hardware has yet to master. Automated rogue blocking is a dangerous endeavor without good categorization. Deploy a Wireless IPS that can reliably distinguish between innocent neighbors, personal hotspots, and network-connected rogues that represent a true threat, taking policy-based action to trace, block, and locate the latter, not just to identify but also to successfully mitigate rogue APs.

Wireless Intruders: Wireless intrusion prevention systems (IPS) as Motorola AirDefense, AirMagnet, and AirTight can detect hostile Wi-Fi clients in or near a company's airspace. WIPS sensors that are up to date and appropriately installed are required for fully effective defense. 802.11a/b/g sensors, in particular, need to be upgraded to monitor new 5 GHz channels (including 40 MHz channels), parse 802.11n protocols, and detect new 802.11n assaults. Furthermore, because 802.11n clients can connect from a greater distance, WIPS sensor location must be reconsidered to meet both detection and prevention requirements.

Mis-configured APs: Configuration failures constituted a substantial security issue when isolated APs were separately handled. To minimize TCO, increase dependability, and reduce risk, most business WLANs are now centrally managed, with coordinated upgrades and frequent audits. However, 802.11n introduces a plethora of somewhat complicated configuration choices, the effects of which are greatly dependent on the capabilities of (extremely varied) Wi-Fi clients. The arrangement and breakdown of multi-media adds to the complexity of setup. To decrease operator error, combine sound, centralized management techniques with 802.11n/WMM teaching and planning.

Ad Hocs and Soft APs: Risky peer-to-peer ad hoc connections that bypass network security safeguards have long been possible with Wi-Fi laptops. Fortunately, few people were driven to utilize ad hocs since they were so difficult to set up. Unfortunately, new laptops with Intel and Atheros Wi-Fi adapters and "soft APs" in Windows 7 are removing this barrier. These virtual APs can provide users with simple, automatic direct connections, bypassing network security and relaying traffic onto the enterprise network. IT-managed client settings and WIPS, which are used to combat Ad Hocs, may also be useful against illicit Soft APs.

Misbehaving Clients: Clients who purposefully or inadvertently make unauthorized Wi-Fi connections harm themselves and their company's data. Some firms use GPOs to set up authorised Wi-Fi connections and prevent end-user changes. Use host-resident agents or WIPS to monitor Wi-Fi client behavior and terminate risky connections. Many enterprises (especially SMBs) still require end-users to connect only to certified wireless APs. Widespread deployment, better reach, and deeper consumer electronics integration have made accidental or incorrect Wi-Fi connections easier than previously.

Endpoint Attacks: Wi-Fi endpoints are being targeted by attackers as over-the-air encryption and network-edge security have improved. Several flaws in Wi-Fi drivers have been exploited to execute arbitrary instructions, sometimes at the ring 0 level, via buffer overflows (high-privilege kernel mode). To initiate Wi-Fi endpoint attacks, automated attack tools like Metasploit can be used. Despite the fact that vendors (usually) fix these vulnerabilities once they are discovered, Wi-Fi driver updates are not automatically supplied with OS upgrades. WiFi endpoint vulnerabilities may be tracked by utilizing WiFiDEnum and Wi-Fi drivers must be updated to keep your employees safe from hackers.

Evil Twin APs: Using the same network name (SSID) as a legitimate hotspot or enterprise WLAN, fraudulent access points can readily advertise to nearby Wi-Fi clients, allowing them to join their network. Because of the proliferation of Evil Twins, which are hacking tools that are simpler to use, your odds of encountering one have increased. Tools such as Karmetasploit can now listen for nearby clients, figure out which SSIDs they're willing to connect to, and then automatically advertise those SSIDs to the rest of the world. When clients join, their traffic is routed to the Evil Twin via DHCP and DNS, where local (fake) Web, mail, and file servers 16 are used to launch man-in-the-middle attacks on the network.

Wireless Phishing: Wi-Fi users are still being tricked by hackers, despite the man-in-the-middle attacks that have already been disclosed. It is possible to poison Wi-Fi client browser caches, for example, if an Evil Twin is used at an open Wi-Fi hotspot to gain access to a previous Web session. After leaving a hotspot, poisoned clients can be redirected to phishing sites even when connected to a wired business network. To reduce this danger, you can clear your browser's cache when you close the browser and start it again. The deployment of an authenticated VPN gateway to carry all hotspot traffic is an alternative (including public). The Wi-Fi network can be monitored and protected by a few open source audit tools that are accessible in order to be aware of these hazards. Using a wireless network, we'll go through a number of them and their features.

1.5 Objective

In this thesis work we are going to examine the performance in various scenarios. There are three scenarios in our work.

- Perform a practical evaluation of the security of IEEE 802.11 wireless networks.
- Auditing networks with the right tools.
- Find out the technical challenges.
- Discuss the future trends based on experimental result.

1.6 Expected Outcome

The goal of the study is to check the performance and the security of wireless lan network. With this work we will get an analysis result based on our experiment and simulation. The experimental result will indicate the types of security threats which have still not been resolved by IEEE 802.11. The works will gives an overview of the several open source network and security analyzing tools.

CHAPTER 02
BACKGROUND

2.1 Introduction

Wi-Fi networks have spread around the globe in a short amount of time. Universities, cybercafé offices, hotels, shopping malls and airports are all places where you'll see it. A wireless adapter-enabled device can connect to the internet through an access point. However, wireless mediums are always subject to security flaws, offering a significant risk to both the developer and the customer.

2.2 Related Works

Since the introduction of smartphones and other mobile devices into everyday life, personal wireless networks have grown in popularity. The 802.11 specifications have facilitated the growth of wireless networks. Low costs and extensive access to both wireless equipment and broadband internet have fueled Romania's expanding number of wireless networks. [4].

Some security holes in wireless networks have been discovered that can be used by criminals to get access to the network or encrypted communication data, despite the continuous extension of 802.11 requirements. Security suggestions are regularly ignored by users despite the fact that vulnerabilities and exploits have been made public. The application of outdated security standards or the inability to fix weak points in access points exposes users to security hazards.

The progress of wireless security in Romania is determined using data from a previous study [5] released in 2012. We also analyze statistics on the presence of well-known attacks and exploits in Romanian personal wireless networks to uncover weaknesses that allow them to succeed. Users who are unaware of the security problems when operating a private network will continue to make poor security decisions, such as using the WEP protocol for authentication or using the equipment's default SSID.

De-authentication and open Telnet access were used to bring down the Bebop UAV and the Parrot AR, respectively, at Defcon 23, according to the author of [4]. As part of our approach, we use the Telnet application to send malicious Java script objects (JSON) over port 44444, but we don't log in to the UAV's telnet server or kill any processes.

Using a Raspberry Pi, Perl script, and free software, security researcher Samy Kamkar was able to de-authenticate a Parrot AR Drone from its controller. Programs could control the UAV in flight using this way. [6, 7]. Known as "Skyjack," this attack utilizes a de-authentication mechanism to gain access to the Wi-Fi on the UAV.

Parrot AR UAV 1.0 and 2.0 were found to be vulnerable to ARP (Address Resolution Protocol) poisoning, as well as DHCP (Domain Host Configuration Protocol) poisoning, according to the author of [8]. While this attack is comparable to ours, we think that we have shown that the newer Parrot Bebop UAV is susceptible to ARP Cache poisoning for the first time. Prior assaults have shown that Parrot Wi-Fi-based UAVs are vulnerable. A large number of these issues were discovered on the previous ARDrone platform. The Bebop platform is the only one we've hacked. Bebop also has the same ARP Cache Poisoning vulnerability as the previous UAV platform, according to our analysis. Additionally, we've uncovered a brand-new vulnerability, the ARDiscovery process, on the Parrot UAV platform that's never been publicly published before. UAVs that are commercially available are unlikely to be developed or manufactured in a secure manner, placing the public at risk if they are utilized at large scale without proper security controls, according to previous studies and the zero-day vulnerabilities we uncovered.

2.3 Research Summary

Here we can see the requirements for establishing a successful Wi-Fi zone. We can readily employ open source tools to ensure wireless network security, and open source technologies can meet all of the requirements stated previously.

2.4 Scope of the problem

Free Software audit tools may also be used to audit wireless networks in the academic sector, such as universities, colleges, and schools. Based on our findings, we recommend that all academic network administrators employ PRTG and wireshark to monitor the wi-fi zone. So that they can be aware of what is going on on their network. Following that, in order to ensure security, they might implement appropriate wireless communication measures.

CHAPTER 03

RESEARCH METHODOLOGY

3.1 Introduction

Wi-Fi hotspots often frequently targeted by hackers. When a free Wi-Fi hotspot is introduced, a slew of other "free" Wi-Fi networks appear, guaranteeing to provide you with web Surfing. Typically, they are bogus Wi-Fi hotspots that urge to be duped into signing into their systems. Personal and sensitive stuff is stolen as user log in. Clients that join to these "public" connections are at high risk of being subjected to a "channeling" assault. "Channeling" is a typical tactic used among cybercriminals to execute man-in-the-middle cyberattacks with the goal of collecting user names, passwords, and other confidential material supplied by the user, and it is a simple task for the attacker.

3.2 Research Subject and Tools:

Since our main goal is analyzed the wifi network for ensuring security, here we have used these analysis tools

- Wireshark to sniff network
- Kismet to test passive sniffing
- PGRT a network monitoring software
- Ettercap Man-in-Middle attack security tool
- NetSpot WiFi analyzer and wireless survey tool

3.3 Data Collection Procedure

To do this work we collected data form online sources, various articles and journals. In this domain there need lots of research's. People's privacy and data security is the buzz word now, we have to ensure the security.

3.4 Implementation Requirements

To finish this work we need these things in our environment.

Sl	Name	Purpose
1	Wireshark	Network packet analyzer
2	Kismet	Wireless Monitoring Software
3	PRTG	Traffic Monitoring Software
4	Ettercap	Network security tool
5	NetSpot	WiFi analyzer and wireless survey tool
6	PC	For Run Software's
7	Wireless Connection	Analyzing Field
8	Linux OS	For Run linux based softwere

Table 1: Implementation Requirements

CHAPTER 04

EXPERIMENTAL RESULT AND DISCUSSION

4.1 Introduction

Each packet sent through Wi-Fi connections includes pieces of information which are used to keep the multiple levels of communication operational. Even though Wi-Fi packets are encrypted, they nevertheless retain unencrypted headers. Anyone examining the network will find the headers useful. The whole MAC (Media Access Control) frame depicted in the preceding graphic is easily accessible to Linux user-space programs. The MAC frame format is used by all packets in a Wi-Fi network. The Frame Management field indicates the type of content that is transported by the MAC frame. There really are three major types of packets, as well as several subclasses.

4.2 Experimental Results

Wireshark: The simplest way to keep tabs on the data being sent and received between protocol units is with a packet sniffer. A packet sniffer captures (sniffer) packets from a computer, as well as storing and/or displaying the information of the different protocol elements in these captured messages. Packet snooping is a passive process. In the background, it keeps track of the messages that other programs and protocols send and receive, but it never sends any packets itself. The packet sniffer is never explicitly addressed in received packets, either. If you're looking for a way to gather data from your device, you'll need a packet sniffer.

Since a command-line ui is really not for everyone, GUI alternatives that also depend on the Libpcap package have indeed been available for a while. Wireshark, that goes back to 2006, is another one of those tools. It was once called as Ethereal, and so many admins are presumably familiar with that term. Because Ethereal developer Gerald Combs departed Ethereal Software, the utility was changed when version 0.99.1 of Wireshark was published. He developed a new project with CACE Technologies called Wireshark, prompting Ethereal Software to suspend production of the prior product.

The Wireshark team now maintains the majority of Wireshark. The open source projects Ethereal and Wireshark are both legitimate open source projects, however Ethereal is aimed toward commercial network analysis tools.

Wireshark is a program that can catch network packets (both input and output) and display them in a graphical user interface (GUI) with complete information about each recorded packet. This application is incredibly useful for network managers who want to discover which machines are attempting to interact with a system. Furthermore, while diagnosing any connectivity-related issue, the information offered by wireshark capture is quite beneficial.

Protocol implementers also use this tool to determine whether or not protocol packets are correctly created. Wireshark is also used by software engineers for debugging whenever they want to know how a packet got on the wire and if it was altered by a program or not.

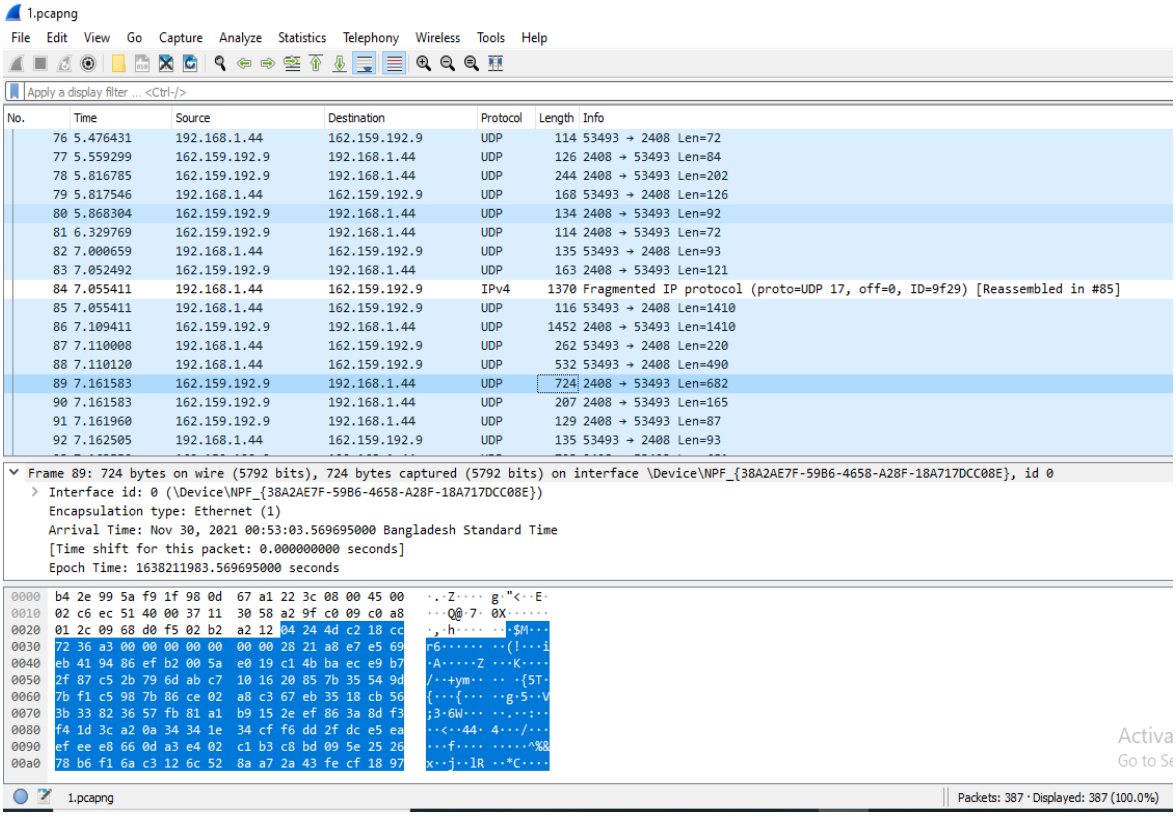


Figure 4.1: Packet sniffing

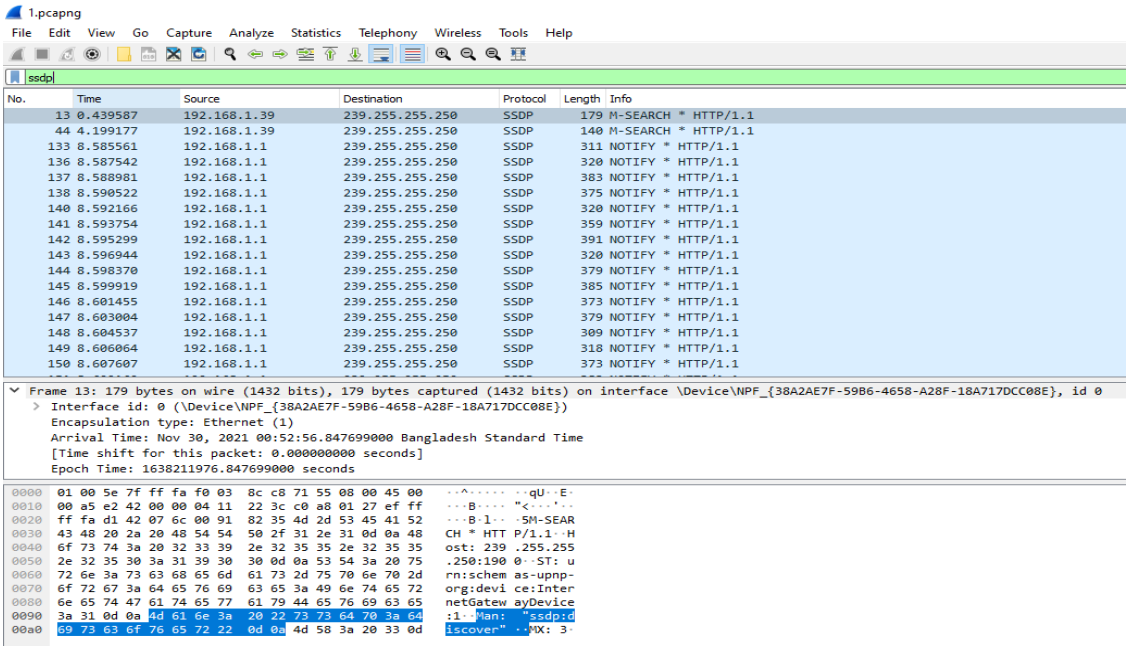


Figure 4.2: Data searching

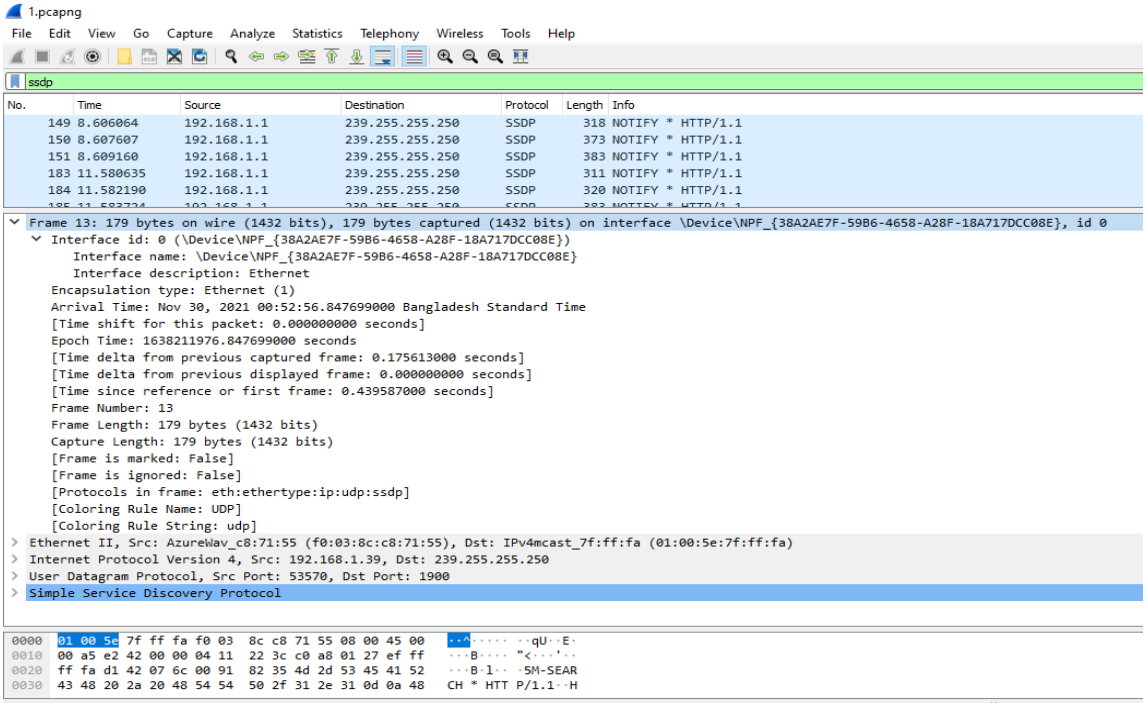


Figure 4.3: Frame analyzing

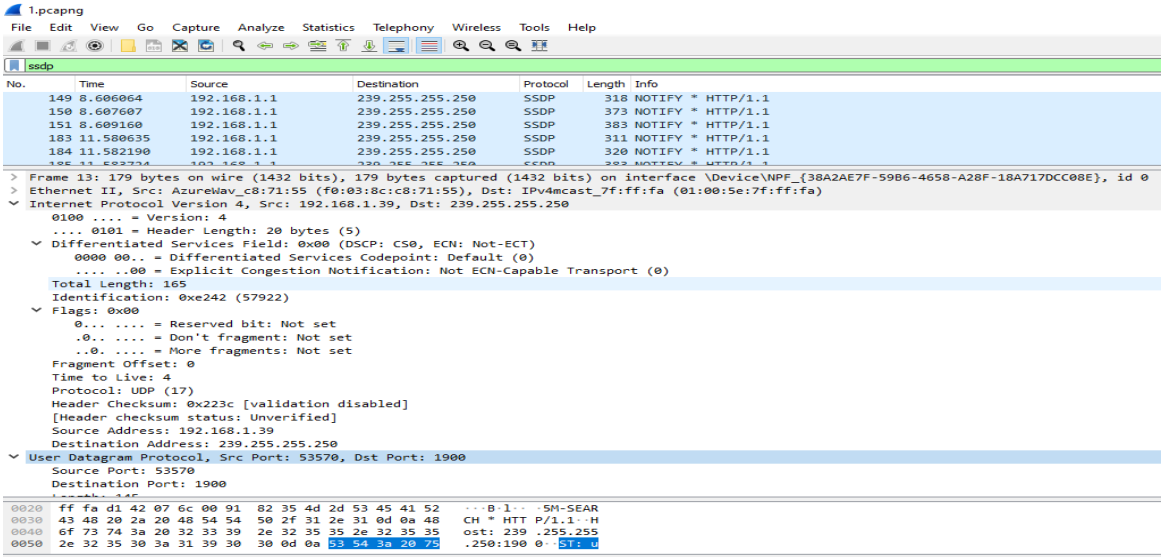


Figure 4.4: Internet Protocol

Kismet: Wireless network analyzer Kismet operates on Linux, Unix, and Mac OS. In the immediate vicinity, it is capable of detecting any 802.11 a/b/g wireless networks. The 802.11 a/b/g protocols are part of WLAN (Wireless Local Area Network) specifications. Kismet has the ability to detect data that other free software does not.

If you want to connect to an unlimited number of servers, you can use the "kismet server" and "kismet client" software.

Many other log files can be generated by Kismet including "dump," csv," and xml files. A GPS device and the "gpsd" program can be used to identify entry points and wireless coverage zones on maps such as Google Maps. Also, "Sox" and "Festival" can be used to play audio alarms and read out network summaries when a problem is discovered. passive sniffer Kismet does not send a lot of packets. As a result, Kismet uses a wireless client adapter that has been put into RF monitor mode. It is impossible to attach the wireless client to any entry point while in "rfmon" mode. Instead, it keeps tabs on every bit of wireless transmission. As a result, your wireless card won't be able to connect to the internet while under Kismet supervision.

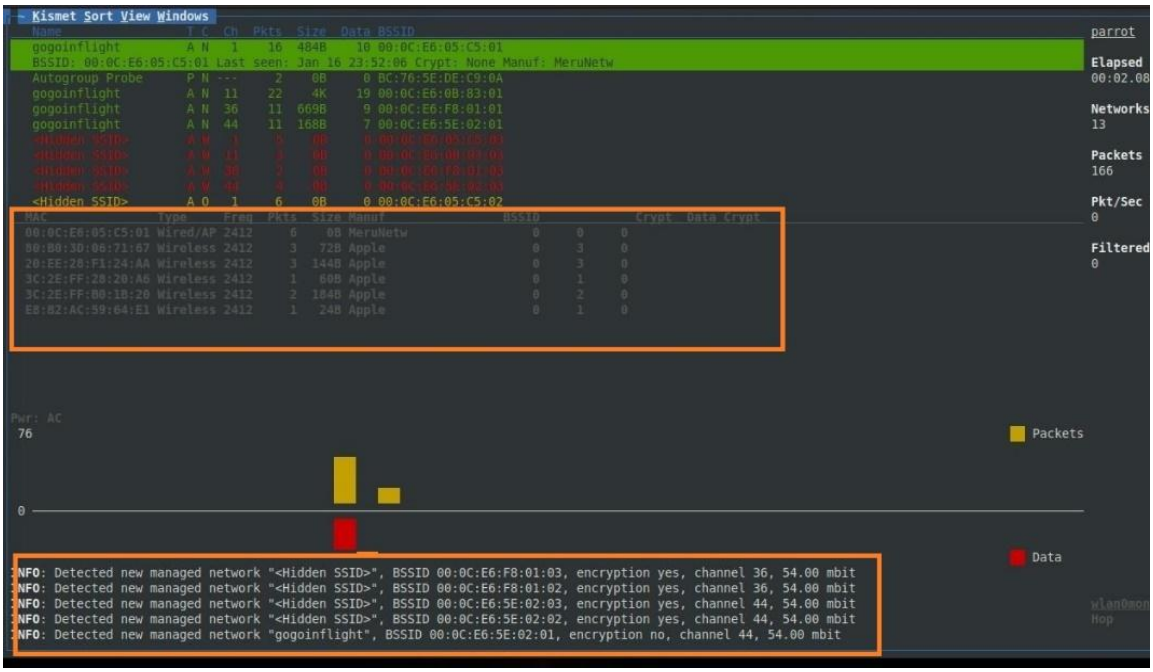


Figure 4.5: Kismet

Ettercap: Ettercap is an abbreviation for Ethernet Capture. Ettercap is a network security feature for LAN man-in-the-middle threats that is free and open source. It may be used to analyze computer network protocols and perform security audits. It may run on a variety of Unix-like operating systems, including Linux, Mac OS X, BSD, and Solaris, as well as Microsoft Windows. It is capable of monitoring network data, collecting credentials, and performing active eavesdropping on a variety of standard procedures.

Ettercap operates by configuring the network interface to be promiscuous and ARP poisoning the target workstations. As a result, it can operate as a "man in the middle" and launch a variety of attacks on the victims. Ettercap allows plug-ins, allowing the functions to be expanded by adding new plug-ins. The attack occurs when one machine requests that the other machines determine the MAC address linked with an IP address. The pirate will respond to the client with bogus packets claiming that the IP address is connected with its own MAC address, thereby "short-circuiting" the true IP - MAC identification response from another site.

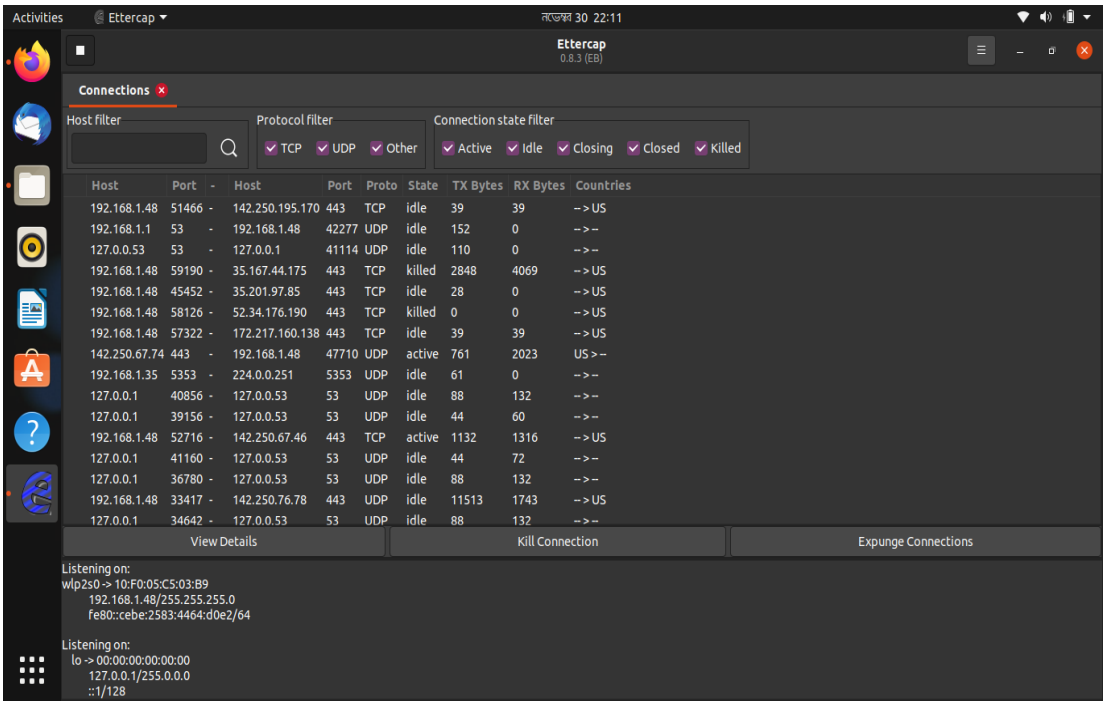


Figure 4.6: Ettercap Connections

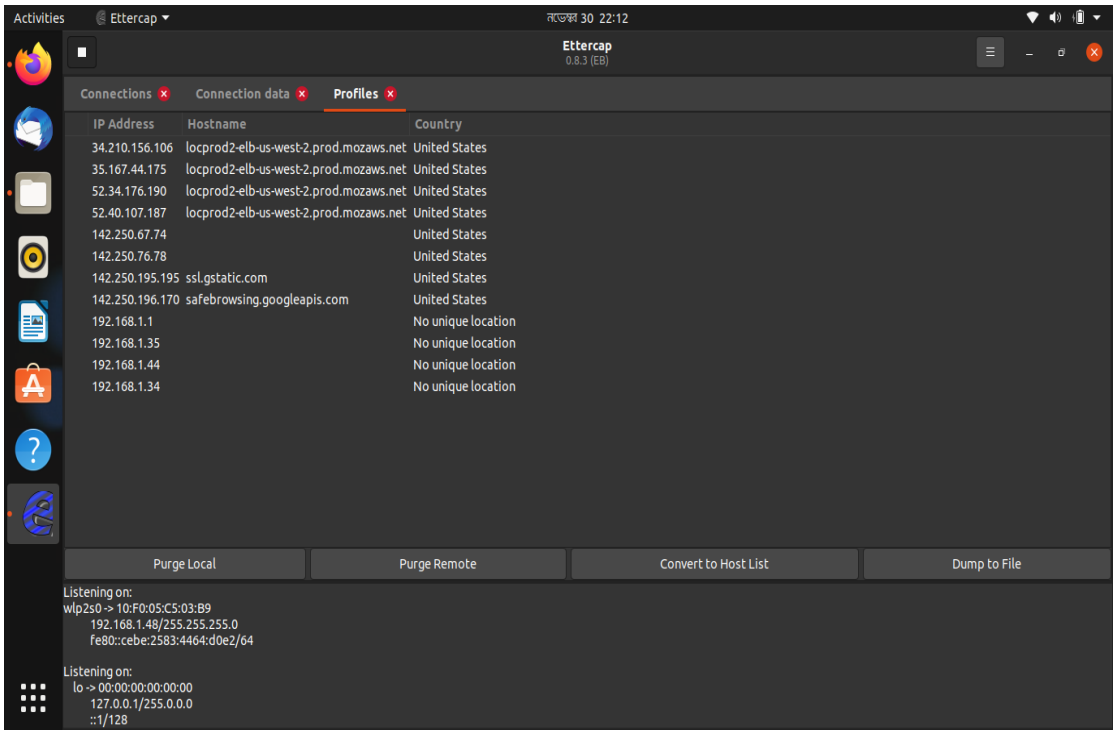


Figure 4.7: Ettercap Profiles

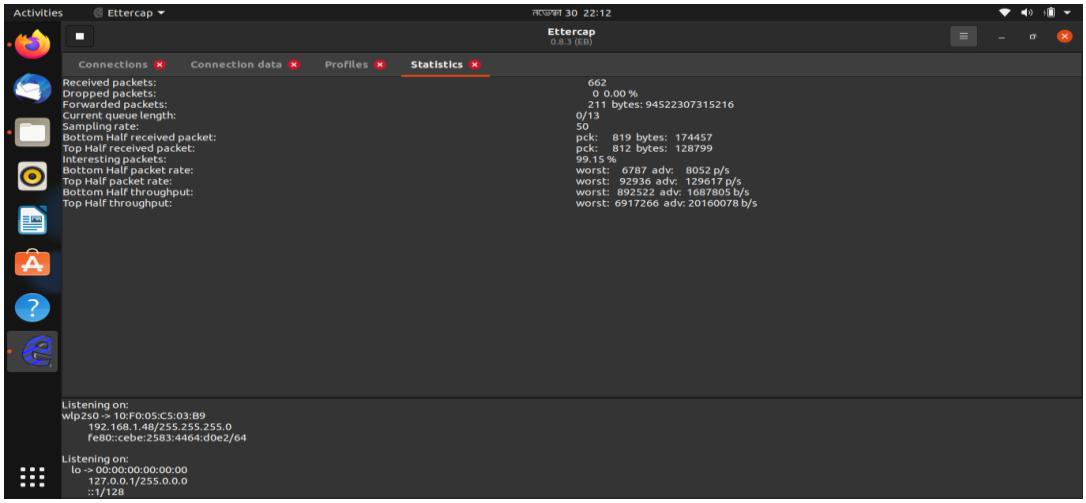


Figure 4.8: Ettercap Statistics

PRTG: PRTG is an application framework evaluation tool, there must be some distinguishable tracking sensors to provide an overview of the network.

PRTG Network Monitor includes a number of sensors, including as SNMP, Netflow, and Sensor, that make it simple to monitor any system's security. Firewall Tracking may be used to see what is occurring with one's internet connection in live time.

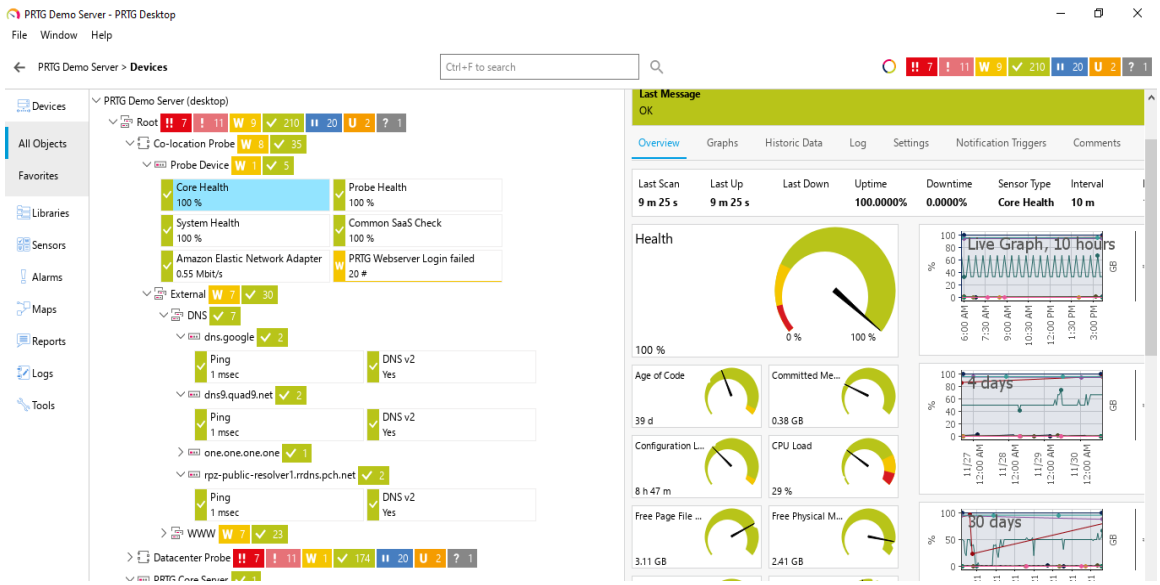


Figure 4.9: PRTG

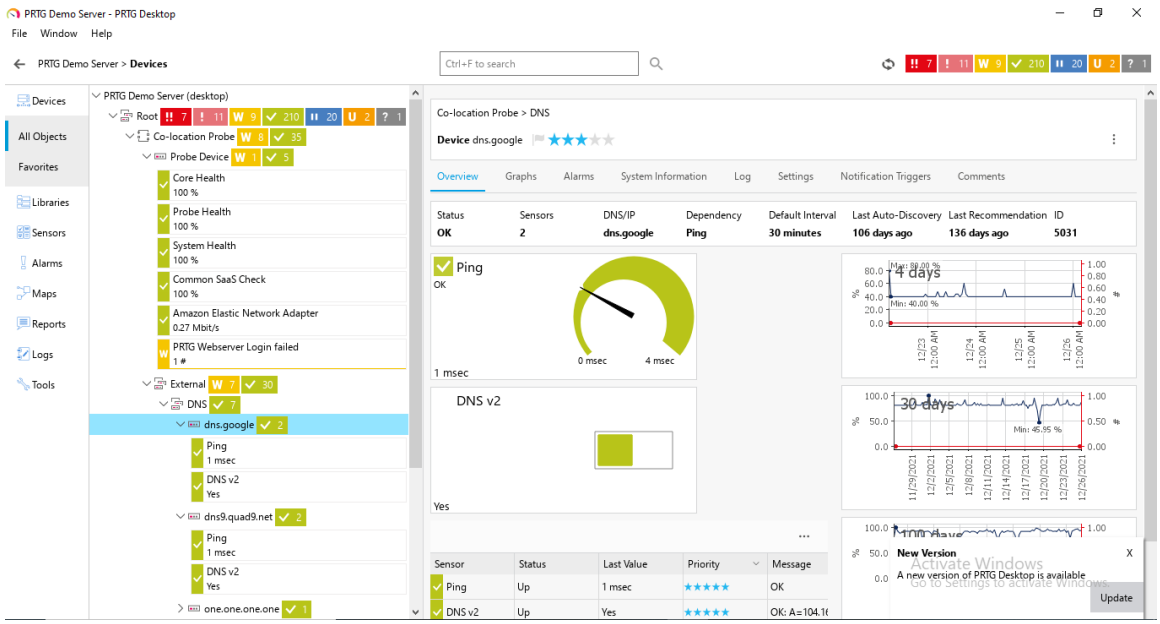


Figure 4.10: PRTG Analysis

Within a network, packet sniffing is used to collect and record information flow. Packet sniffing makes it possible to identify and analyze individual packets based on predetermined parameters. Packet sniffing enables extremely thorough network monitoring and bandwidth use assessment. Nevertheless, in order to grasp the significance of the data being watched, a wider understanding of networks and its inner workings is required.

NetSpot: Network administrators of all skill levels can use NetSpot's user-friendly interface. Discovery and survey are the two modalities of action. An overview of local Wi-Fi networks appears in the first mode; the survey mode displays more comprehensive Wi-Fi strength heat maps.

Setting up NetSpot is a cinch, and it comes with a slew of graphic representations of the wireless spectrum and the data it can gather. There are four options: free, home, commercial, and enterprise. Differences include how many zones you can view, how many access points you can scan, and the number of data points you can collect from a scan.

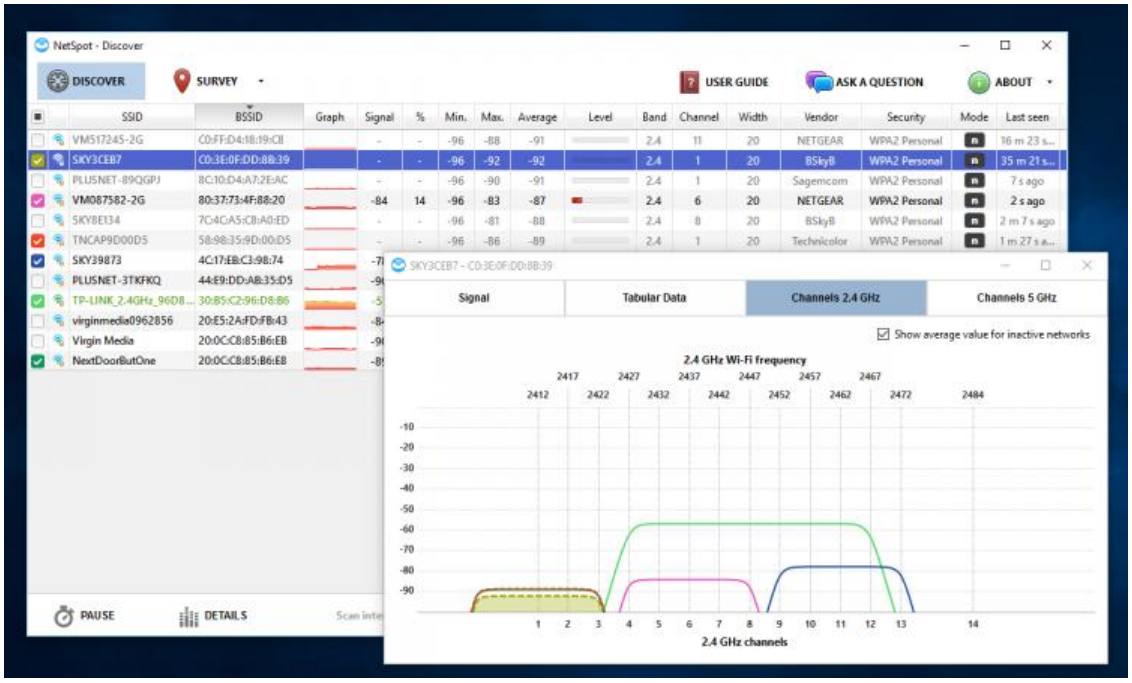


Figure 4.11: NetSpot

4.3 Peer-to-peer Network Security Using Wireshark

A P2P network's security framework is depicted in Figure 4.12. The various users demonstrate that any gadget and/or human can be a network peer. Wireshark was launched as a network monitoring tool to help assess and safeguard the network by capturing and analyzing all data communication. After analyzing, the security implications of P2P networks can be better understood.

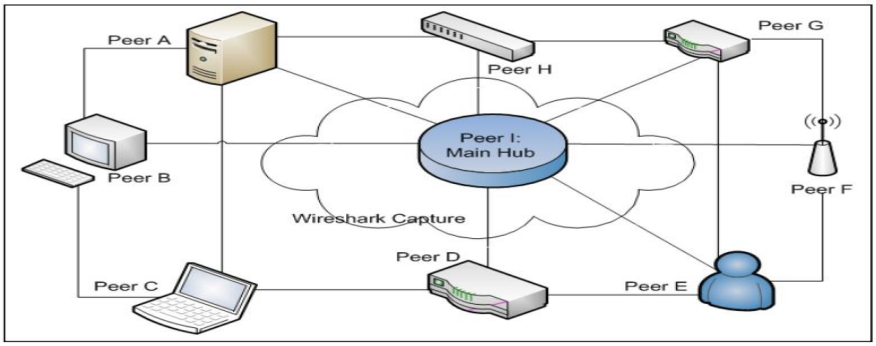


Figure 4.12: Diagram of Peer to Peer Security

It's critical to have a thorough understanding of peer-to-peer networking in order to grasp the security implications in a peer-to-peer environment. We need to know, for example, that security features are available in traditional client/server networks but not in peer-to-peer networks. It's also important to understand the limitations of peer-to-peer networks. These constraints will assist us in comprehending the distinctions between the two networking systems. When it comes to networking, both systems follow a similar procedure.

A computer network is made up of at least two workstations, at least one shared resource, and a way to connect the computers (typically an Internet Router or Ethernet). A server is used in some popular types of networks, such as client/server networks. In a traditional client/server network, the server houses all of the allocated resources. For example, if a database needs to be accessed from multiple workstations, it would be located on a server in a pure client/server environment.

A peer-to-peer network operates in a completely different way. A client/server network is built for small organizations or a small working group of individuals within a larger organization, whereas a peer-to-peer network is designed for small organizations or a small working group of people within a larger organization. Although there is no definite limit to the number of clients that can participate in a peer-to-peer network, the practical limit is 10. When a peer-to-peer network grows to more than 10 machines, performance and administrative challenges are likely to arise. This is due to the fact that a peer-to-peer network is intended to be the simplest type of network. There is no centralized server in charge of controlling shared resource access. Rather, the resources are stored on the users' local devices. As a result, the network in Fig. 1 had nine users for greater functionality. The goal of the security feature added to the P2P network environment, Wireshark monitoring, is to acquire access to reliable network information. Network forensics is another name for network forensics.

Network Forensics:

Monitoring and analysis of network traffic as well as trace and log data of network intrusions acquired by the network security tools currently running in the system are the primary responsibilities of network forensics[26].[27] An investigation can be carried out by analyzing the evidence it gathers. Network data and protocol characteristics can be collected using a variety of security and forensic techniques. In order to preserve the evidence, the data collected can be stored in any file format.

In digital investigations, passive and active evidence collecting are typically divided into two subcategories: Network traffic can be used to gather forensic evidence in the form of passive evidence gathering. Evidence is gathered through active interaction with other stations on the network, which can be done either by being a part of the conversation on the network or by listening in on the communication. Passive evidence gathering for the acquisition of forensic evidence on P2P networks is the topic of this investigation.

Wireshark and the uTorrent BitTorrent client were used in this experiment to show how a packet sniffing tool can monitor a P2P network. It's possible to download files using BitTorrent using UTorrent. Most people have heard of BitTorrent because of this program. As with BitTorrent, each peer wishing to download a file must be able to communicate with other Bittorent clients and share files with other currently active peers in order for UTorrent to function properly. uTorrent includes a distributed hash table (DHT) as part of its basic client feature. The distributed hash table (DHT) helps keep track of which peers are currently utilizing each client, as well as which files they are sharing. For this study, we used uTorrent because it is said to be 16 percent quicker than other clients on average.

The goal of this investigation was to identify the digital evidence remnants left behind by BitTorrent peers on a Windows 7 PC during the communication or downloading of a suspected file. Wireshark was used to capture and analyze the file as a packet sniffer.

The second step's objective was to record all of the communication between the BitTorrent client and other peers, both inbound and outbound. It is at this point that the investigator launches the BitTorrent software and begins searching for the file.

Sniffer and capture all network traffic in the fourth step of the process this would provide us the opportunity to look for network artifacts in the collected traffic and probe the network.

- A Windows 10 PC running the most recent version of UTorrent and Wireshark (v2.6.6) were used for the experiment.
- A torrent tracker was requested 377 times.
- A series tracker called 'Condor,' which we found on a torrent site, has been installed.

The next step in our experimental setup was to get things going. A clean experimental environment was maintained by restricting the system to only having uTorrent and Wireshark running. Wireshark was launched first, and it was given permission to begin recording. UTorrent and the 'Condor' tracker were both started concurrently. This ensured that all network traffic between the uTorrent client and other clients carrying the 'Condor' file was captured in full detail. When the file had finished downloading, the capture ended.

After the file had finished downloading in figure 2, Wireshark began displaying the peers connected to download the file. Peers' IP addresses and BitTorrent clients are being displayed in a panel for the first time, which is a success. One of the most important pieces of information for a digital investigator is the identification of other people who are interested in the suspected file.

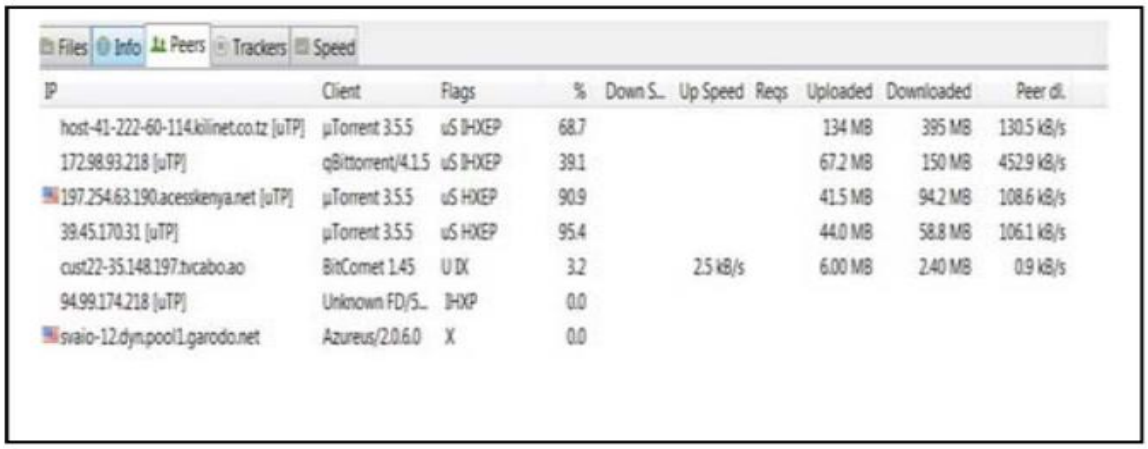


Figure 4.13: Peer to Peer

Threats: Because peer-to-peer harmful threats still require access to the system's current workstation, user authentication can guard against the insider danger. Authentication, on the other hand, may not be the best way to security in the future.

Network scanning and monitoring may become more desirable if peer-to-peer networking becomes standard in corporate computing infrastructures and universities[30]. Such scanning is not straightforward since, by definition, peer-to-peer data transfer does not go through a central server, such as an Amazon server. Network scanning technologies like Wireshark, as well as regular Forensic Data Analysis of collected data, may be beneficial in preventing hostile threats from utilizing peer-to-peer data that passes inside and outside of businesses. However, companies must exercise caution when selecting a peer-to-peer networking architecture, as the Invisible Internet Project (I2P) paradigm will render networking investigation ineffective because all data is encrypted.

4.4 Summary

The majority of commercial establishments, hotels, and governmental organizations that see WiFi hotspot connectivity as a crucial network function is growing. , When it comes to giving staff access to LAN programs, fostering client involvement, and supporting guest Internet connectivity, WiFi connectivity is vital to these companies' capacity to run theirbusinesses.

CHAPTER 5

SUMMARIZATION OF THE STUDY AND CONCLUSION

5.1 Summary

Wi-Fi-only networks are progressively being installed by younger multi-location enterprises; no Ethernet connection is run. In such circumstances, the business must evaluate the dependability of each location's connectivity to centralized assets and design a Wi-Fi architecture that meets network accessibility and dependability needs while remaining within a tiny budget.

On multi-location Wi-Fi networks, it is common for various users to just have varying access safety requirements. Employees require the technical standards for Wi-Fi protection, 802.1X-based accessibility, whereas clients profit from the establishment of a captive platform with sign-on splatter. A multi-location business needs to ensure that its Wi-Fi architecture allows for both worker and guest access, and that the appropriate level of security is enabled for each.

5.2 Conclusion

We did our best to explain the utility of several excellent free source tools for wireless network audits. As a result, network administrators and IT administrators may utilize open source tools in conjunction with existing manual processes and software applications to scan wireless networks and safeguard them from unwanted hacking. Wi-fi is becoming a fairly widespread technique of connecting to a broadband connection in multi-location commercial enterprises. The majority of offices disclose intelligence via a wi-fi network. If WPS availability is enabled, it may be vulnerable to a virtualized assault. If the IT department (System Administrator) in the banking industry does not stay updated with the latest segment of network traffic, they may risk undesired hacking.

To address these issues, Free Software Audit tools should be implemented as part of the safety system process. As a result, we recommend that they use Ettercap and Kismet to audit their network. Open Source audit tools may also be used to audit wireless networks in the academic sector, such as universities, colleges, and schools. Based on our findings, we recommend that all academic network administrators employ PRTG and wireshark to analyze the wi-fi zone. So they can be aware of what is happening on their network. Following that, in order to ensure security, they might implement appropriate wireless network measures.

References

[1] Y. Wen and T. Liu, "WIFI Security Certification through Device Information," 2018 International Conference on Sensor Networks and Signal Processing (SNSP), 2018, pp. 302-305, doi: 10.1109/SNSP.2018.00065.

[2] H. Peng, "WIFI network information security analysis research," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp. 2243-2245, doi: 10.1109/CECNet.2012.6201786.

[3] H. Peng, "WIFI network information security analysis research," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp. 2243-2245, doi: 10.1109/CECNet.2012.6201786.

[4] F. Campoccia, M. L. Di Silvestre, E. Riva Sanseverino and G. Zizzo, "Analysis of the efficacy of a WiFi architecture for the management of Medium Voltage distribution systems," 45th International Universities Power Engineering Conference UPEC2010, 2010, pp. 1-6.

[5] A. Zafft and E. Agu, "Malicious WiFi networks: A first look," 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 1038-1043, doi: 10.1109/LCNW.2012.6424041.

[6] H. Zhong and J. Xiao, "Design for integrated WiFi defence strategy in mordern enterprise context," 2014 IEEE 5th International Conference on Software Engineering and Service Science, 2014, pp. 748-753, doi: 10.1109/ICSESS.2014.6933675.

[7] A. Sebbar, S. Boulahya, G. Mezzour and M. Boulmalf, "An empirical study of WIFI security and performance in Morocco - wardriving in Rabat," 2016 International Conference on Electrical and Information Technologies (ICEIT), 2016, pp. 362-367, doi: 10.1109/EITech.2016.7519621.

[8] H. Peng, "WIFI network information security analysis research," 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp. 2243-2245, doi: 10.1109/CECNet.2012.6201786.

[9] M. Hooper et al., "Securing commercial WiFi-based UAVs from common security attacks," MILCOM 2016 - 2016 IEEE Military Communications Conference, 2016, pp. 1213-1218, doi: 10.1109/MILCOM.2016.7795496.

[10] A. Zafft and E. Agu, "Malicious WiFi networks: A first look," 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 1038-1043, doi: 10.1109/LCNW.2012.6424041.

[11] H. Qu, J. Cheng, Q. Cheng and L. Y. Wang, "WiFi-Based Telemedicine System: Signal Accuracy and Security," 2009 International Conference on Computational Science and Engineering, 2009, pp. 1081-1085, doi: 10.1109/CSE.2009.60.

[12] Bin Tian et al., "A novel key management method for wireless sensor networks," 2010 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), 2010, pp. 1106-1110, doi: 10.1109/ICBNMT.2010.5705261.

[13] Y. Wang, J. Lu, Z. Wu and Y. Lu, "Component Based Security Control for Information Network," The Proceedings of the Multiconference on "Computational Engineering in Systems Applications", 2006, pp. 1357-1360, doi: 10.1109/CESA.2006.4281849.

[14] T. Yin, L. Han, C. Wan, X. Qu and Y. Li, "The Probability of Trojan Attacks on Multi-level Security Strategy Based Network," 2010 International Conference on Multimedia Information Networking and Security, 2010, pp. 555-559, doi: 10.1109/MINES.2010.122.

[15] Z. Qu and X. Wang, "Study of Rough Set and Clustering Algorithm in Network Security Management," 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009, pp. 326-329, doi: 10.1109/NSWCTC.2009.47.

[16] J. Li and C. Dong, "Research on Network Security Situation Prediction-Oriented Adaptive Learning Neuron," 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010, pp. 483-485, doi: 10.1109/NSWCTC.2010.247.

[17] M. Astekin, S. Özcan and H. Sözer, "Incremental Analysis of Large-Scale System Logs for Anomaly Detection," 2019 IEEE International Conference on Big Data (Big Data), 2019, pp. 2119-2127, doi: 10.1109/BigData47090.2019.9006593.

WIRELESS LAN SECURITY ANALYSIS FOR IEEE 802.11 AND ITS TECHNICAL CHALLENGES, RECENT ADVANCES, AND FUTURE TRENDS

ORIGINALITY REPORT

25%	22%	1%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dspace.bracu.ac.bd:8080 Internet Source	14%
2	Submitted to Daffodil International University Student Paper	2%
3	computer.howstuffworks.com Internet Source	1%
4	Submitted to Australian Institute of Higher Education Student Paper	1%
5	Submitted to Lancers International School Student Paper	1%
6	Michael Hooper, Yifan Tian, Runxuan Zhou, Bin Cao, Adrian P. Lauf, Lanier Watkins, William H. Robinson, Wlajimir Alexis. "Securing commercial WiFi-based UAVs from common security attacks", MILCOM 2016 - 2016 IEEE Military Communications Conference, 2016 Publication	1%