**A Project Plan on**

**Security and Privacy Model of Next Generation Intelligent Network**

**Submitted to**

**Amity University Uttar Pradesh**



**In partial fulfillment of the requirements for the award of the degree**

**Of**

**Bachelor of Technology in**

**Computer Science and Engineering**

**By**

**ARYAN RAWAT**

**A2305219448**

**Under the guidance of**

**Dr. Sunil Kumar**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**AMITY SCHOOL OF ENGINEERING AND TECHNOLOGY**

**AMITY UNIVERSITY UTTAR PRADESH**

**DECLARATION**

I, Aryan Rawat student of B. Tech (CSE) hereby declare that the project titled “Security and Privacy Model of Next Generation Intelligent Network” which is submitted by me to Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, in partial fulfillment of requirement for the award of the degree of Bachelor of Technology in Computer Science , has not been previously formed the basis for the award of any degree, diploma or other similar title or recognition.

**Date: -** 30.6.2021

**Name: -** Aryan Rawat

**Roll No: -** A2305219448

Name and signature of Student(s)

Aryan Rawat

**CERTIFICATE**

On the basis of declaration submitted by Aryan Rawat, student(s) of B. Tech CSE , I hereby certify that the project titled “Security and Privacy Model of Next Generation Intelligent Network” which is submitted to Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida, in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering, is an original contribution with existing knowledge and faithful record of work carried out by him/them under my guidance and supervision.

To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Noida

Date 05-07-2021

Department of Computer Science

Amity School of Engineering and Technology

Amity University Uttar Pradesh, Noida

**ACKNOWLEDGEMENT**

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with success. I would like to thank Prof (Dr.) Sunil Kumar Name, Head of Department-CSE, and Amity University for allowing me to undertake this project. I would like to thank my faculty guide Mr. Sunil who is the biggest driving force behind my successful completion of the project. She has always been there to solve any query of mine and also guided me in the right direction regarding the project. Without her help and inspiration, I would not have been able to complete the project. Also, I would like to thank my batch mates who guided me, helped me, and gave ideas and motivation at each step.

**Aryan Rawat**

**A2305219448**

5CSE-7X

Contents

[1. INTRODUCTION 7](#_Toc77165294)

[2. MY IDEA OF IMPLEMENTATION 8](#_Toc77165295)

[3. NEXT GENERATION NETWORK 8](#_Toc77165296)

[3.1 Eight security and privacy dimensions used in NGN.Fig.1. 8](#_Toc77165297)

[3.2 Structure of next generation network 11](#_Toc77165298)

[4. how a connection is established 13](#_Toc77165299)

[5. COMMON ATTACKS TO BREACH SECURITY AND PRIVACY 14](#_Toc77165300)

[5.1 Distributed Denial of Service 14](#_Toc77165301)

[5.2 ARP poisoning 16](#_Toc77165302)

[5.3 Packet sniffing using Wireshark 17](#_Toc77165303)

[6. TOOLS OR SOFTWARE MODELS WIDELY USED FOR SECURITY AND PRIVACY 17](#_Toc77165304)

[6.1 VPN and Leased lines 17](#_Toc77165305)

[6.2 Security onion 18](#_Toc77165306)

[6.3 Tracking Tools 19](#_Toc77165307)

[6.4 Data-encryption 20](#_Toc77165308)

[6.5 Firewall 21](#_Toc77165309)

[7. IMPLEMENTATION 22](#_Toc77165310)

[8. CONCLUSION 33](#_Toc77165311)

[9. REFERENCES 34](#_Toc77165312)

**ABSTRACT**

Due to development in technology in NGN there is also a spike in security and privacy data breach which can be related to stealing data bases of big social networking websites or shutting down websites for important resources. This advancement has led to a considerable increase in cyber related crimes. There are many ways to counter these problems and protect yourself from attacks which already exist in security and privacy structure of NGN. In this paper we will discuss about, proper explanation of NGN and aspects involved in security and privacy, different types of attacks and tools used, various existing protocols, functions and methods which protects hosts all over internet.

Lastly, we will perform a synflood attack to capture the SYN packets using Wireshark and analyze what all information we can get. We will also list ways to protect yourself from these attacks which are discussed in paper.

# INTRODUCTION

Due to the rising need of network systems, networks are continuously upgrading, becoming faster and complicated mainly from the security point of view. The statistical data show all vulnerabilities and attacks increasing making the general threat getting more common. We need to understand the working of New Generation Networking to understand the flaws of it and how people exploit it. NGN as defined by ITU-T (international telecommunication union- responsible for introducing NGN in main stream media) as “packet-based network able to provide services including telecommunication services and able to make use of multiple broadband, quality of service – QoS enabled transport”. One of the distinct feature of NGN is that the service related functions are separated from the underlying transport related technologies [1] [2].

Due to the digitization whole data was forced to be turned into digital form which increased the data breach and stealing of data as well as depending on networking for faster sharing data. According to a census conducted there are 3.4 billion smartphone users in the world. CISCO blocked 7 trillion cyberattacks and potential threats that's 20 billion attacks each day. Including invasion of privacy, wire threats, money laundering, false identity enrollments of domain names, espionage, theft of highly classified treaties, DDoS attacks, and other crimes — which put a huge burden of money loss on governments and individuals scaling to around tens of billions dollars [3][4].

There is a large scope for attacks as everything around us is approachable through internet and attackers analyze the working of networking and exploit the resources. Due to lack of knowledge normal people can easily be targeted.

Challenges [5]:

- Every new NGN service contains new and different compositions of different types of technological devices and software. Therefore it has more different kinds of risks related to components, for example the PSTN, and its protocols are still used for VoIP.

- Major errors and flaws arise due to oversight in designing IP.

- Basic network mechanism of network can be used to steal data or interrupt working of system.

# MY IDEA OF IMPLEMENTATION

Perform a vulnerability attack on network for record purpose and use tools like Wireshark to capture packets and see how actually we can prevent them.

# NEXT GENERATION NETWORK

An interconnection of various devices, called as hosts that are connected using multiple ways for the purpose of sharing and receiving of data. This is known as a network of devices [6].

It known as a packet-based network that supports mobility and can be used for both telecommunication and data services. It has the ability to take advantage of various broadband services, particularly Quality of Service (QoS) stacked transport technology, in which the service-related operations are decoupled from the transporting technology [7] [8].

## Eight security and privacy dimensions used in NGN.Fig.1.

1) The security dimension of access control

The security aspect of access control defends against unauthorized use of network assets. Access control confirms that simply authorized people or maneuvers are permitted to access network features, stockpiled information, info flows, and facilities. In top of that RBAC role based access control gives multiple level of permits to ensure only some individuals and devices could be accessed and execute tasks on network subsets [9] [10].

2) Authentication security dimension

The authentication security dimension is used to approve the identity of interactive entities. Authentication certifies the rationality of confirmed identity of the units involved in the communication (for example, a being, device, facility, or request) and ensures that a unit does not attempt to tamper or rerun a preceding statement [11].

3) The security dimension of non-repudiation

The security dimension of non-repudiation delivers means to prevent a person or unit from opting for a certain act regarding the information by providing proof of different linked activities to the network (such as proof of obligation, intention or commitment; proof of origin of data, proof of ownership, proof of use of resources).It makes sure to avail some kind of evidence which can be shown to third part organization as a proof of certain type of act that has taken place [12].

4) Data privacy dimension

The data privacy aspect safeguards data against unauthorized exposure. Data Privacy guarantees that information content cannot be decoded by unauthorized objects [13].

Data Encryption, access control lists, and file permissions are commonly used means of ensuring data security.

5) The Communication Security Dimension

The Communication Security Aspect confirms that data is only transmitted between official endpoints (data is not hijacked or interrupted as it travels among endpoints [14].

6) Data Integrity Security Dimension

Data Integrity Security Dimension confirms the accuracy or correctness of data. Information is secured by preventing unapproved adjustment, deletion, formation and copying, and offers a suggestion of such unapproved actions [15].

7) The Availability Security Dimension

The Availability Security Aspect confirms that there is no rejection of approved access to net features, stockpiled data, information flow and different services provided because of acts affecting the net.

8) The privacy security dimension

The privacy security dimension offers protection for data that can be obtained by observing net activities. Examples of this data contains the websites that the user has visited, the customer's physical location, the IP addresses and DNS labels of devices on the service provider's network [16] [17].

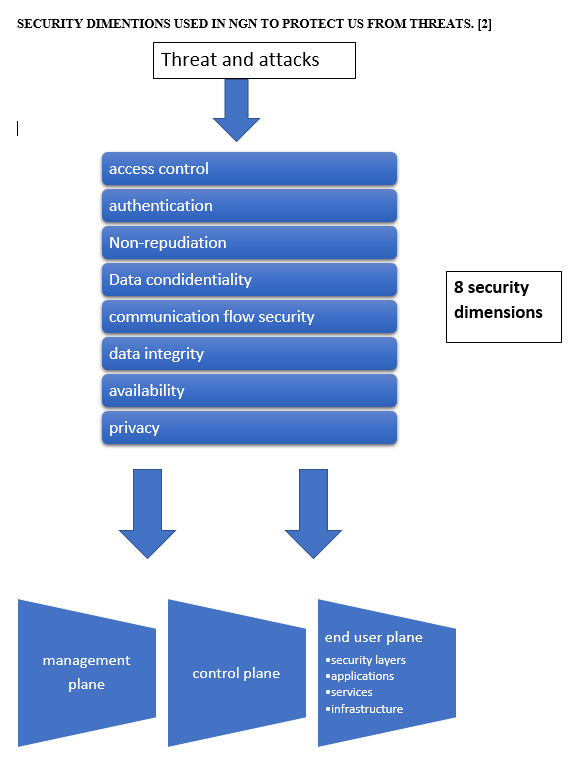


Fig. 1. Security dimensions in NGN

1. Features of Next Generation Networking:

• Wireless networks need nodes that are self-defining and flexible enough to self-organize and self-heal in different situations. It is not possible to use the default infrastructure for exploitation of network management in the temporary network (ad-hoc). This unique feature also represents a major security challenge for the wireless network. If the configuration of the sensor network is lacking, the damage caused by the attack or dangerous environment can be huge [18]

• USE OF PACKETS- The data bits are transferred from location to another in the form of packets which may or may not take same route to reach destination and sometimes does not reach destination which is termed as packet loss [19]

• Goal of NGN is to replace the conventional PSTN (Public Switched Telephone Network) and Integrated Services Digital network (ISDN). These both were a primitive way of sending data, voice and services over network, so NGN introduced a different way to interact with each other [20][21]

## Structure of next generation network

Protocol: it’s a set of rules or integrated algorithms which shows us how two devices can communicate across the network and there many different protocols across each layer of open system interconnection [22].

There are many different protocols used for different purposes which should be known for implementation

* TCP (transmission control protocol)

It is a set of predefined rules that are normally used to interconnect network devices on the internet it chooses how the information will be shared through end to end communications that consists how to organize bundles of data and receiving them by creating channels of communications across a network [23].

* IP (internet protocol)

The IP address tells the packets the address and routes used so that they reach correct destination several packets may have same destination address but different routes.

* UDP (user datagram protocol) alternate of TCP

UDP is basically used as an alternate of TCP protocol. A communication protocol that provides the exchange of data and information between computers on a network. In networking that uses Internet Protocol (IP), it’s usually known as UDP/IP.

* FTP (File Transfer protocol)

You might have heard of FTP, or File Transfer Protocol, but you might not know exactly what it is. Basically, a FTP is a method to facilitate connection two devices together in the most secure way likely to facilitate the transmission of data between two points. If you send the file via FTP, the file will be uploaded or download from a FTP server. When you upload a file, it is transferred from the PC to the main server. When an individual get the files, the files will be sent from the server to PC. TCP/IP (Transmission Control Protocol/Internet Protocol), or the basic language used by the network to execute commands, is used to handover documentations using FTP [24].

* Hyper Text Transfer Protocol (HTTP)

This protocol is made to share hypertext or a preferable display or language for displaying information between two or more systems.

Most of the information shared over network, counting the content of web pages and API calls, all of them generally uses HTTP protocol. Two types of general HTTP messages are 1) requests 2) responses.

* Hyper Text Transfer Protocol Secure (HTTPS)

HTTPs is generally used to transmit information among the client browser which has requested data and the web server which responses the request in hypertext, it’s almost same as in HTTP transmission just in HTTPs transmission is done in an encrypted manner which means the packets carrying data are carrying encrypted information [25][26].

* DHCP- Dynamic host configuration protocol

DHCP (Dynamic Host Configuration Protocolis a network management protocol that is generally used to automatically assign IP while entering networks which allows the devices to use basic services namely DNS and NTP. The DHCP server automatically assigns IP addresses and other net configuration factors to every connected entity on network so that they can share data and info with other IP networks. DHCP servers assigns a unique IP address to the client to work over internet.

* ARP –address resolution protocol is used to link our internet protocol address to media access control address that exists in a local area network. It basically converts the 32 bit long IPv4 into 48 bit long MAC and vice versa for transfer purposes. [27][28]

# how a connection is established

First of all the browser goes to DNS server and gets the actual address of the server on the desired site is located. then the browser at our end sends an HTTP request in the form of message to the server of desired site, asking the server to send an identical copy of the main web page to client then once the server verifies the request it send the client a special message called as “200 ok”, and starts to send the info and data of main web page to browser in series of small distinguished pieces called as the data packets. All these messages and data in the form of packets sent between client and server is shared over our network using TCP and IP protocols. Then the browser on our side starts to assemble all the scattered data packets in the form of webpage which can be understood by the user. The term client used here is just any device connected on internet using web access software’s which are known as web browsers whereas the server is generally a computer with large memory and storage which hosts websites and application.Client and server connects with each other by requests and responses in the form of SYN and ACK packets respectively [29].

# COMMON ATTACKS TO BREACH SECURITY AND PRIVACY

## Distributed Denial of Service

Denial of service (DoS) attack it’s a way used by the attackers to block services provided by the server. It involves overflowing servers with artificial requests generated by malicious computers so that the input of requests becomes more then the server can accept. This leads to overload of server and disruptions in working of server. As a result of this attack the online services provided by the server becomes scarce and the traffic assortment fails. Huge corrupted machineries known as the botnets are made to efficiently perform this attack. The hackers at the point when server is down try to break in through malicious malwares. There is also a sub type of DoS attacks that is DDoS or distributed denial of service attack where more than one source are involved in flooding the server. To stop the working of server hackers choose targets that contain large database on servers and have huge user base, prominent sites such as bank and charge cards are primary targets. Major organizations such as flip cart, Facebook, twitter are major targets for these kinds of attacks because they have a large data base [30].

How to recognize:

* One of the most noticeable feature to detect a DDoS attack is noticing any website or page that you usually visit suddenly becomes slow and start to jitter as these issues can be caused due to general high traffic flow. Further investigation can show exact route of traffic and make it clearer if it is a DDoS attack or not [31].
* Malicious traffic coming through a specific IP address.
* Large amounts of incoming traffic from IPs who share a profile behavior, such as a specific device IP or type, geographic location, or web browser statistics.
* Unknown increment requested for a page or endpoint

Common types of DDoS attacks:

1) UDP flood

UDP flooding is DDoS attack that as name suggests floods a predefined target with User Data Protocol (UDP) packets. The initial purpose of the UDP flood is to flood the open ports on a server. This forces the server to constantly verify for applications that are listening on the particular port, and (when no applications are found) to respond with an "Unreachable destination" ICMP packet. These attacks exhausts the server's resources, which can eventually lead to server closing [32][33].

2) SYN flood

A SYN flood DDoS attack is done generally to exploit a weakness in the networks TCP protocol sequence known as a “three way handshake”. In a three way handshake a SYN request packet is sent by the client to establish a TCP connection with server which should be answered by the server in the form of SYN-ACK response, then acknowledged ACK response from the requestor. In the event of a SYN flood, the attacker acts as a user and try to establish a connection with the target by sending multiple SYN packets from the open ports of the device. The target sends response to as much packets as possible in the form of SYN-ACK packets and receives no response ACK packets while SYN packets keeps on stacking. A saturation point comes when the number of requests overwhelm the CPU and the target system waits for confirmations for each request sent from spoofed IPs, all the other resources are halted until a new connection is established which results in denial of services [34].

3) Ping of death

A deadly ping attack ("POD") consists of an attacker who sends many malicious and malformed pings to a target PC. The official max length of an IP packet is 65,535 bytes. The data link layer usually places a limit on max frame size.in ping of death circumstances a big IP packet is split into several IP packets which is called as fragments and the host gathers the IP segments to make the full packet. In the Ping of Death scenario, after maliciously manipulating fragmented content, the receiver at last ends up with an IP packet bigger than max size of 65535 bytes when recollected together. This as a result overflows the memory buffer which is given for the packet, causing Denial of service for the normal packets [35].

4) HTTP flood

In a HTTP flood, a hacker exploits the general HTTP GET or POST requests to hack or attack a server. HTTP flood do not use malicious packets, impersonation and require much less bandwidth than other known attacks to bring down the targeted PC, server or website. The attack is considered executed or most efficient when it forces the server to allocate as manty resources as possible to satisfy each request. [3]

## ARP poisoning

ARP-poisoning is also called as ARP-spoofing. It’s an attack which is carried in the LAN or local area network that generally consists of sending tampered malicious ARP packets to the default gateway of router in order to change the normal pairings in its IP to MAC address grid. ARP packets are used because Arp protocol is used to translate IP address into MAC address because ARP protocol is made for efficiency and convenience and not for security purposes, they are very easy to execute as long as the attacker has control over any one of the device connected over LAN.

The attack comprises of the attacker sending a malicious ARP response message to routers gateway, which says that its MAC address must be linked with the IP of the targeted device. the default gateway when receive message it broadcast the message to all devices on the network After the default gateway receives this message and broadcasts its changes to all other devices on the network, now all the traffic or data from targets IP to any other device will first go through attackers PC, allowing the attacker breach targets privacy which is also known as packet sniffing [36].

## Packet sniffing using Wireshark

Packet-sniffing is the process of gathering and recording more or less of the packets traveling over a PC network, irrespective of in what way the data packet is addressed. Each package, or a distinct subsection of packages, can be collected together for additional examination. As a web administrator, one can use the recorded information for various uses, such as for monitoring bandwidth and traffic.

A packet evaluator, occasionally referred to as a packet analyzer, consists of two important aspects. First, a network card which links the evaluator to the current network. Second, the software delivers a way to record, display or analyze the recorded data [37].

# TOOLS OR SOFTWARE MODELS WIDELY USED FOR SECURITY AND PRIVACY

## VPN and Leased lines

A leased line is defined as a line connection which offers a devoted connection with plenty of bandwidth usually without proxy or authentication. It’s generally used by big companies who needs connection for whole building or branch.

A VPN connection is way to establish a safe link or tunnel among internet and you. By using a VPN, all the traffic information and data is sent through a special encrypted virtual tunnel. This function easily hides your IP address whenever you are using your internet connection, making your original physical location invisible. VPN connections are as well safe from external attacks. This is due to the encrypted tunnel all the data transferred is transferred through this virtual encrypted tunnel and no one can access the tunnel as they don’t have the key.

VPN are widely used to hide real IP so that while opening unauthorized websites which may record IPs and attack the ip address cannot get the address of the real machine address .it’s also used to access content or stream content which is not available in a particular country by tunneling to a IP address of another country [38].

## Security onion

Security Onion is a well-known open source and free Linux distribution for threat detection, see Fig. 2. Organization security monitoring as well as log management. It includes TheHive, Playbook, Fleet, osquery, CyberChef, and many more security tools which are proved efficient for privacy and security management. [6]

Security Onion flawlessly weaves together three core purposes:

• Powerful analysis tools

• Full packet capture

• Network and endpoint detection.

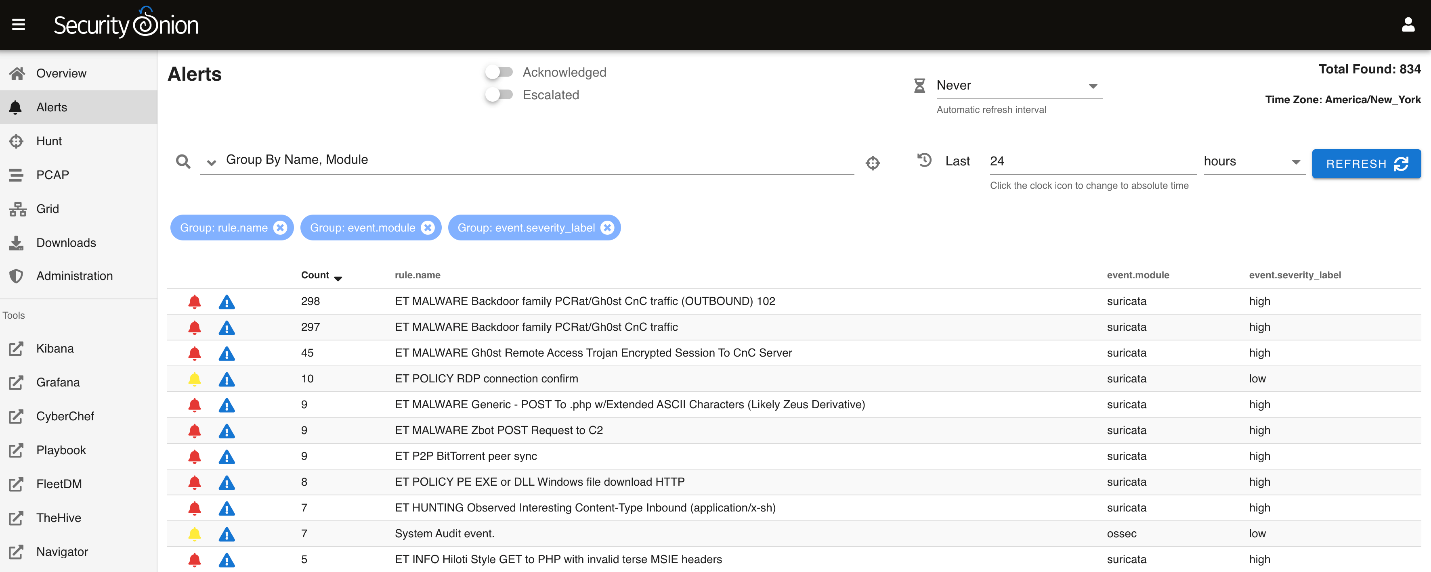


Fig. 2. Security onion interface. [39]

## Tracking Tools

Tools like Wireshark, Fig. 3, prove to be very helpful in analyzing malicious activity over your network. You can get the source IP, the type of packet, time when packet is received. They help to capture all packets flowing through your machine in a network connection in case of attacks like synflood you can easily check the packets receiving at your end and after seeing too many SYN request packets from a single IP address you can block that IP from your router gateway.

Wireshark is the most widely used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1) Capture packets:

Wireshark listens for network connections in real time, then picks up the entire traffic stream - most likely tens of thousands of packets simultaneous.

2) Filtering:

Wireshark can slice and dice all this live random data using filters. By applying filters, you can get only the information you need.

3) Visualization:

Wireshark, like any good packet sniffer, allows you to drill down into the middle of network packets. It also allows you to view the entire conversation and network flow.

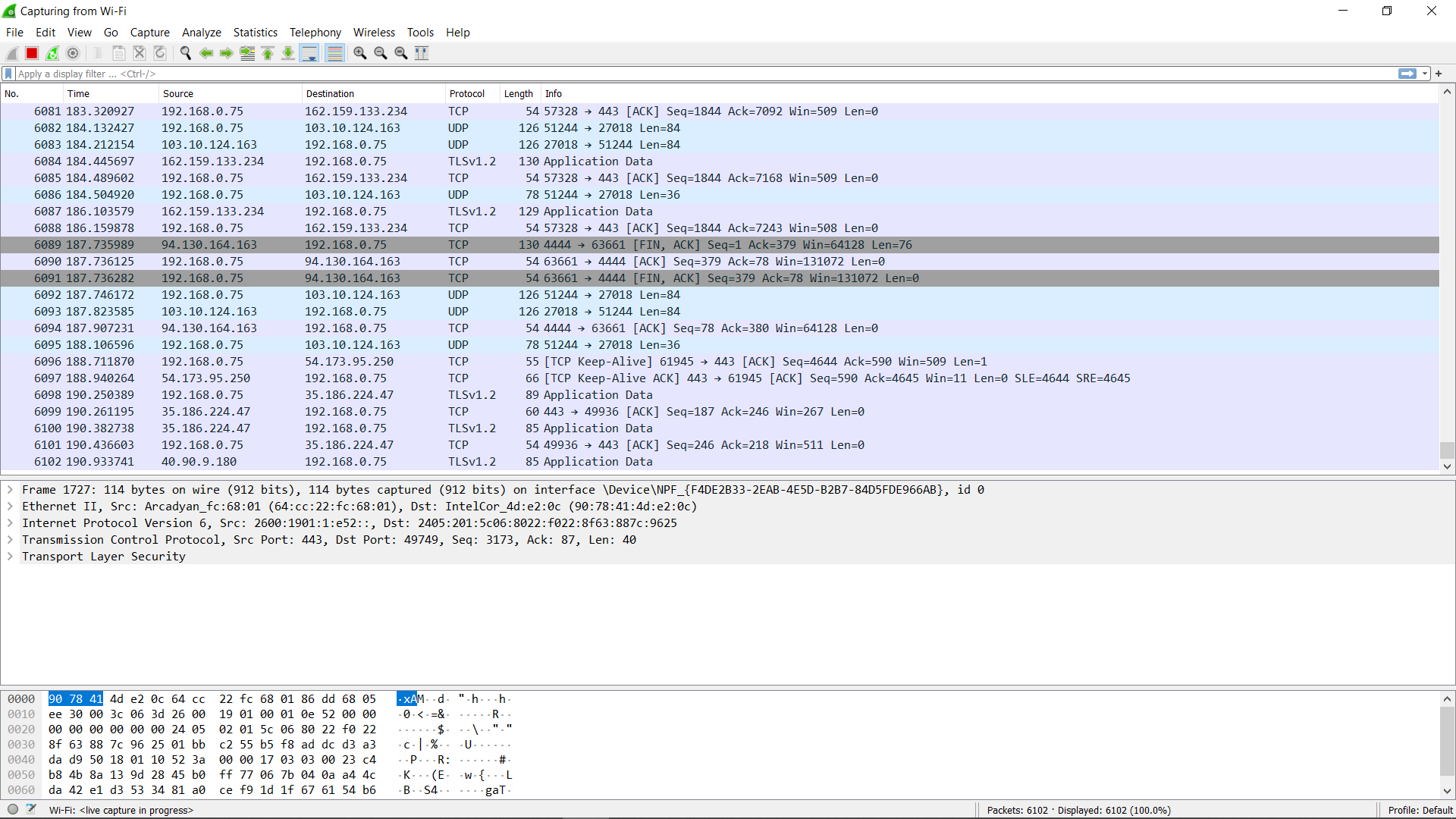


Fig. 3. Wireshark snapshot

## Data-encryption

Data-encryption takes a piece of information and transforms it into a new type that can only be read by those who have access to the key. This key is also referred as cryptographic key. We usually denote encoded data as cipher text and unencrypted data as plain text. The purpose of data encryption is to protect the privacy of information [40]. See Fig. 4. As you can imagine, data protection has developed as a major distress for businesses with volatile evolution in data volumes and workers who are carrying large amount of important confidential business data on their PC, laptop and devices.

As businesses and their staffs also work together with cloud services more often, more and more data moves beyond corporate walls. The propagation of information and the facility to transfer data from one system to another has helped multinationals to achieve today’s business needs.

The major difference between HTTP and HTTPs protocol is that in HTTPs the data in packets is encrypted so the displayed text is not understandable by a third person whereas if someone login in a website while someone capture the packets between that user and web server then they can easily access users login information if HTTP is used. Nowadays normally HTTPs is used everywhere because it’s secure.

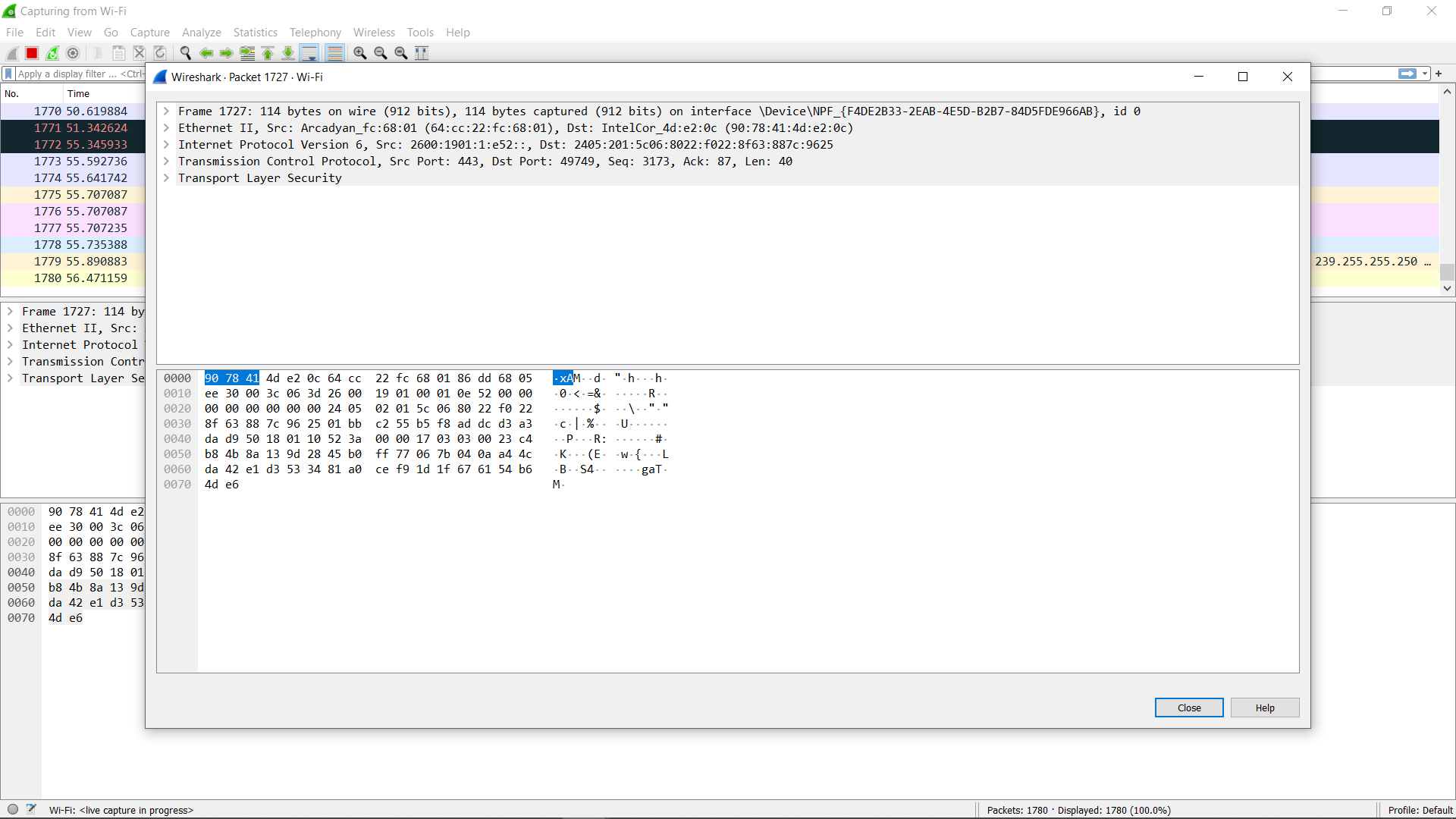


Fig. 4. Snapshot of encrypted data

## Firewall

The Firewalls, particularly new generation ones are focused on the prevention of malware and application layer attacks which we have discussed earlier. Joint with a united Intrusion Prevention System (IPS), these new-generation firewalls can respond rapidly and transparently to notice and battle attacks across the net. They can function based on pre-verified policies to better defend ones network and can accomplish rapid valuations to notice hostile or doubtful activity, such as malware and others. By taking benefit of firewalls for your safety structure, you configure your net with precise rules to permit or block inbound and outbound traffic.

The network layer or packet filter inspects packets at a low status in the TCP/IP protocol stacks, not permitting packets to pass through the firewall if they conform to an established rule set where the source and destination of the Internet Protocol (IP)-based rule set of addresses and ports. Network layer inspection firewalls perform better than similar devices that test the application layer. The downside is that unwanted apps or malware can go through authorized ports, for example. Internet traffic goes using the HTTP and HTTPS web protocols, ports 80 and 443 respectively. That’s why we should always check for open ports on our network side. It also helps to prevent DDoS attacks by closing specific ports through which traffic is coming in.

# IMPLEMENTATION

1) PREPARING TOOLS AND INTERFACE

* We will perform a synflood vulnerability attack from kali Linux interface which is the best tool used for pen testing. I have used windows subsystem for Linux (WSL 2 by Microsoft <https://docs.microsoft.com/en-us/windows/wsl/install-win10>) which have capability to run Linux and windows simultaneously.
* Install Wireshark to capture the syn packet and record them on both target and source machine. Fig. 5.

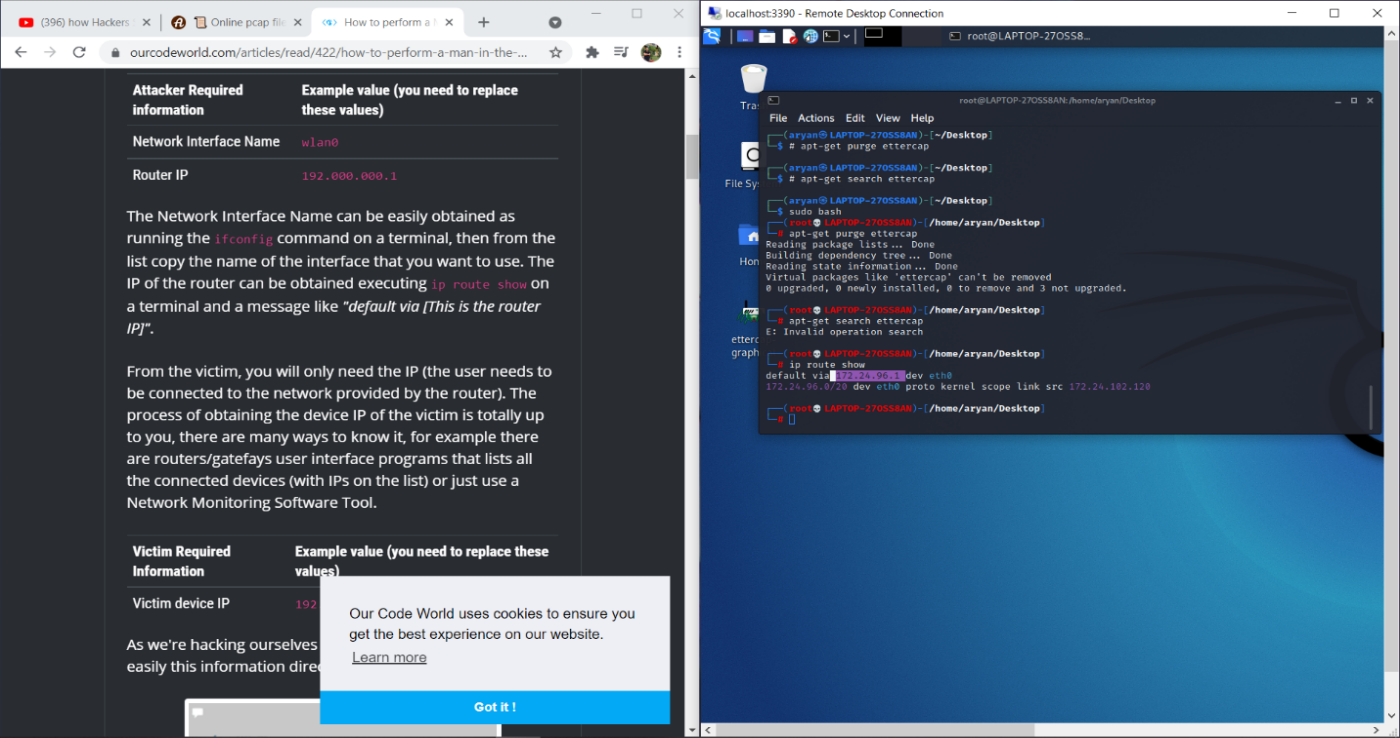
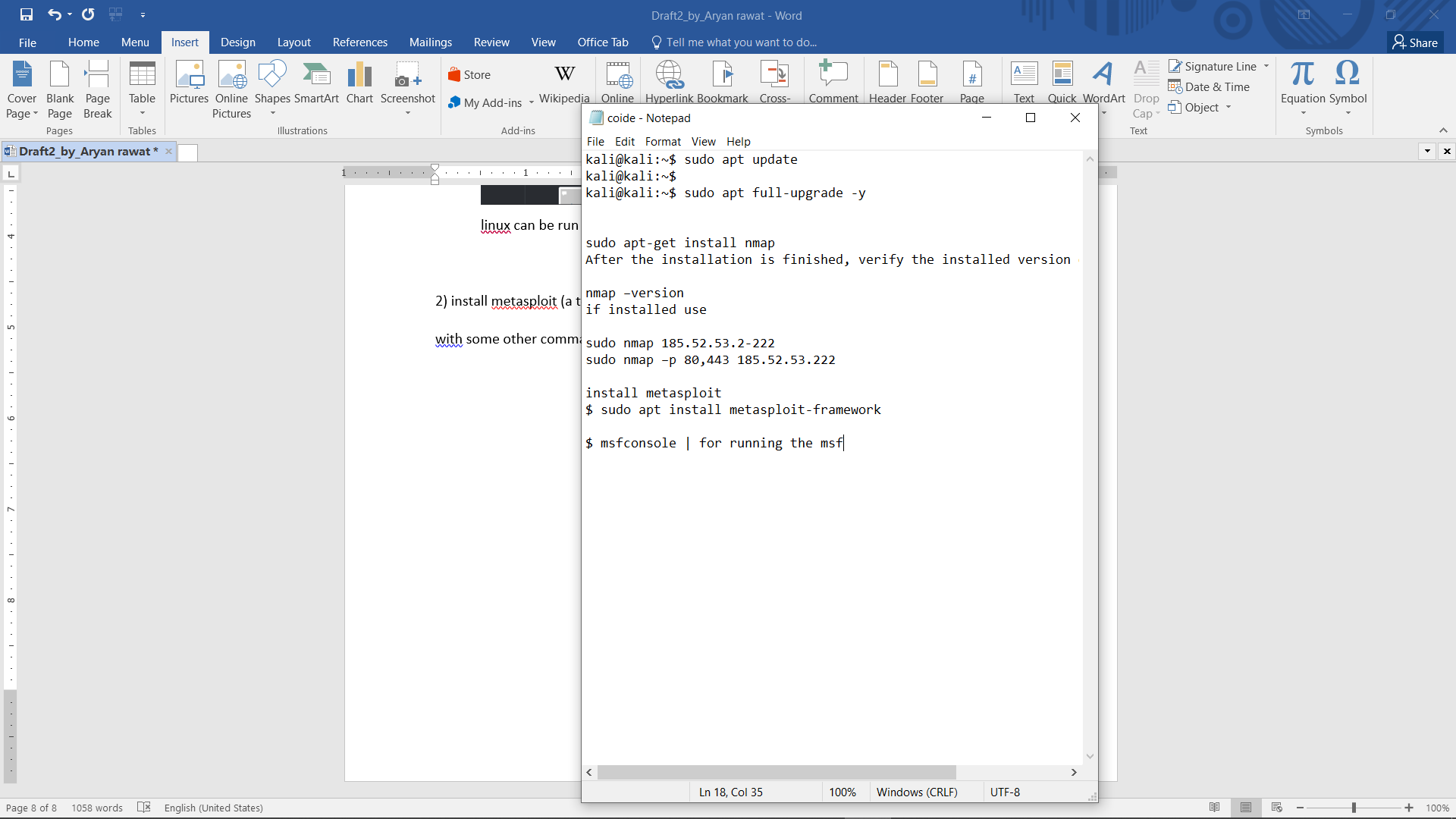


Fig. 5. Windows subsystem for Linux

* Linux can be run with windows in remote desktop connection connected by Ethernet.

2) install metasploit (a tool for exploitation) and nmap (tracking and searching tool)

With some other commands for upgradation see Fig. 5.



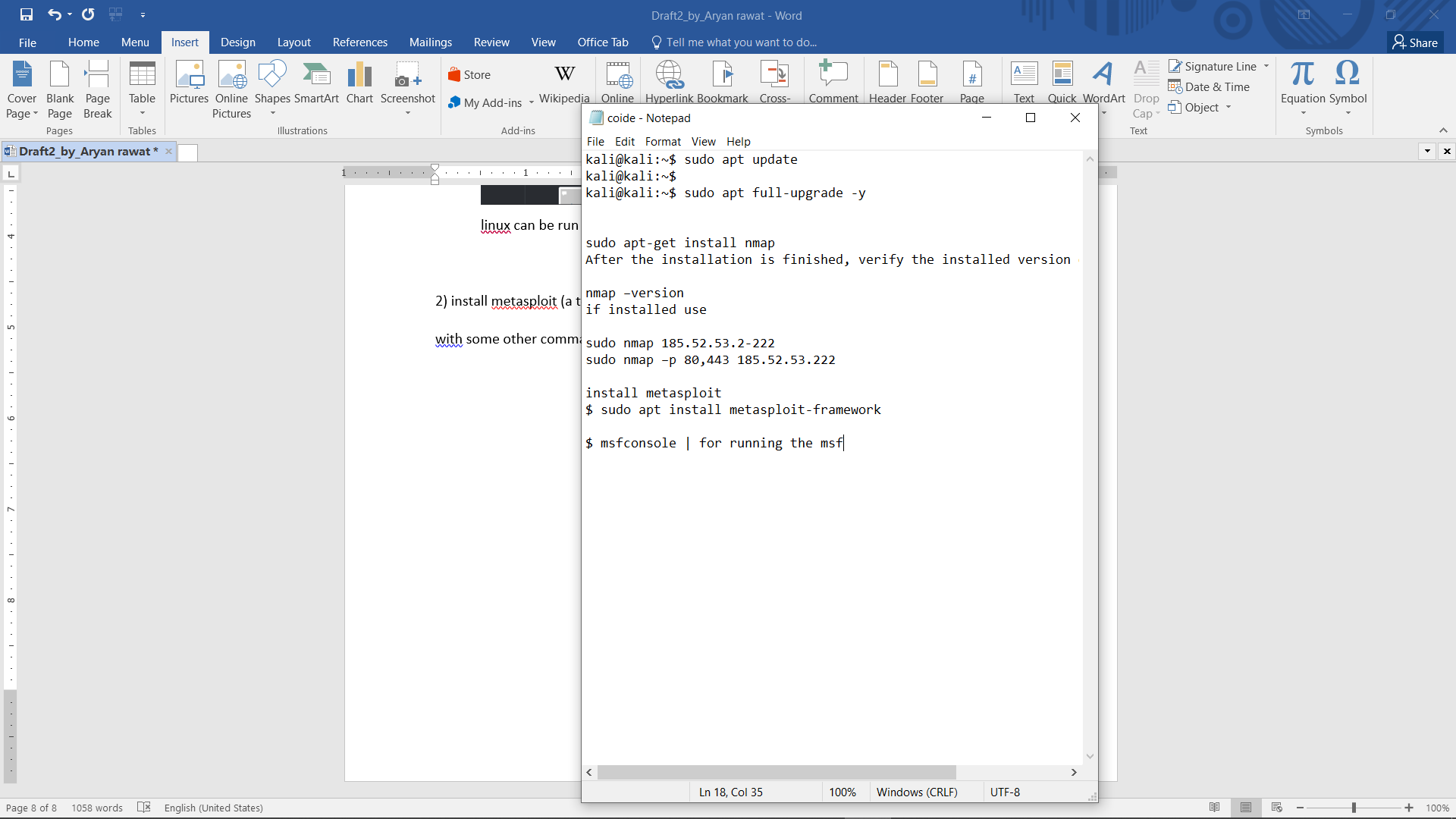


Fig. 5.linux commands

3) Get info about your ip address as well as the network connection which in our case is Ethernet eth0 see Fig. 7.

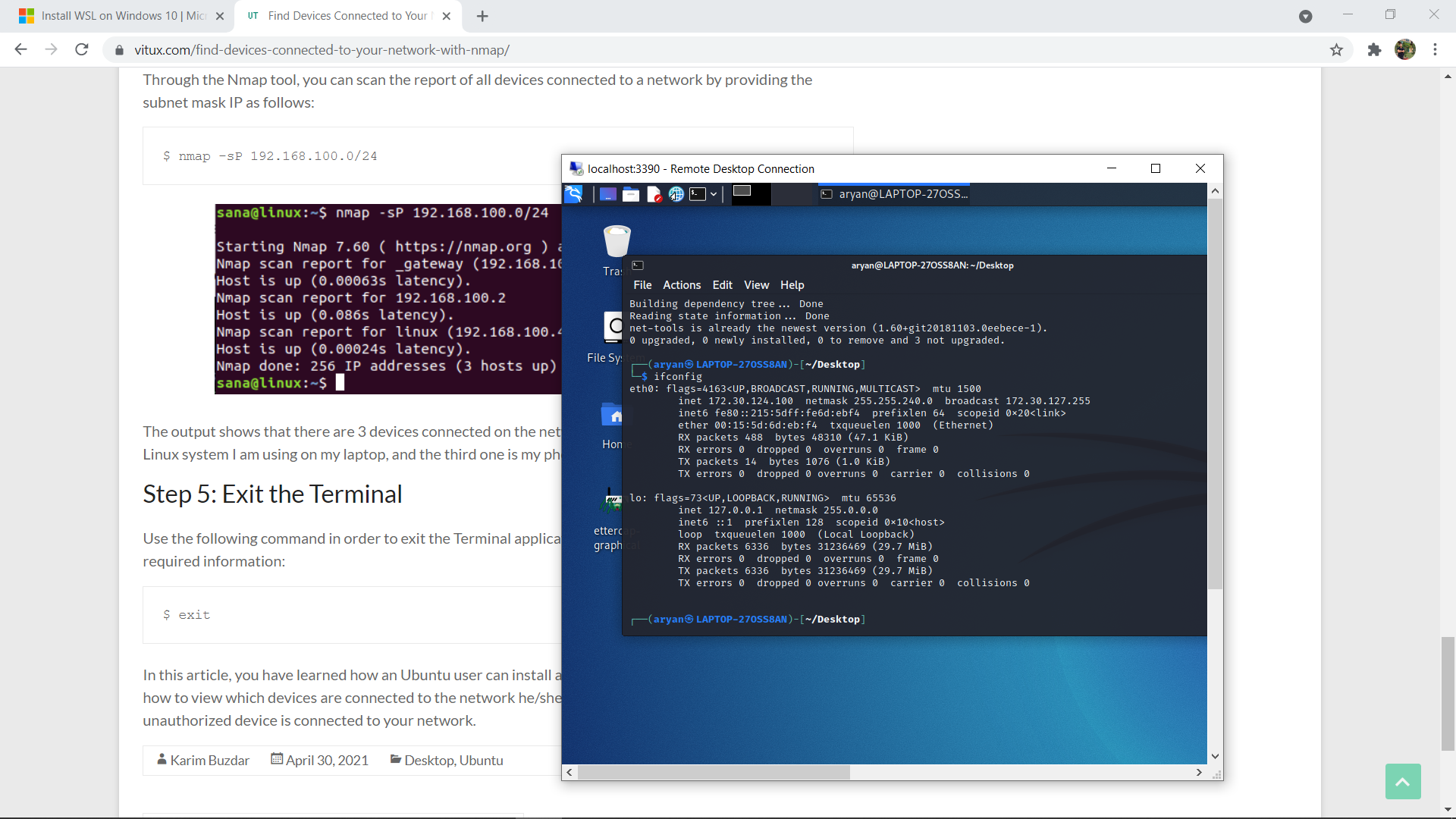


Fig. 7. ip configurations

4) Now scan for devices connected to your network by using given command and choose your target see Fig. 8.

Use your subnet ip mentioned in ipconfig details

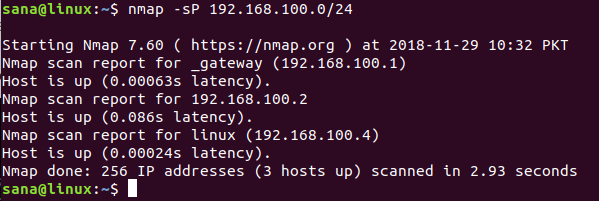


Fig. 8. Nmap network scan

5) This will show you all devices connected to your routers network gateway .Now check your targets IP and use that to check for open ports on that system. These open ports will be used to send traffic to the target system see Fig. 9.

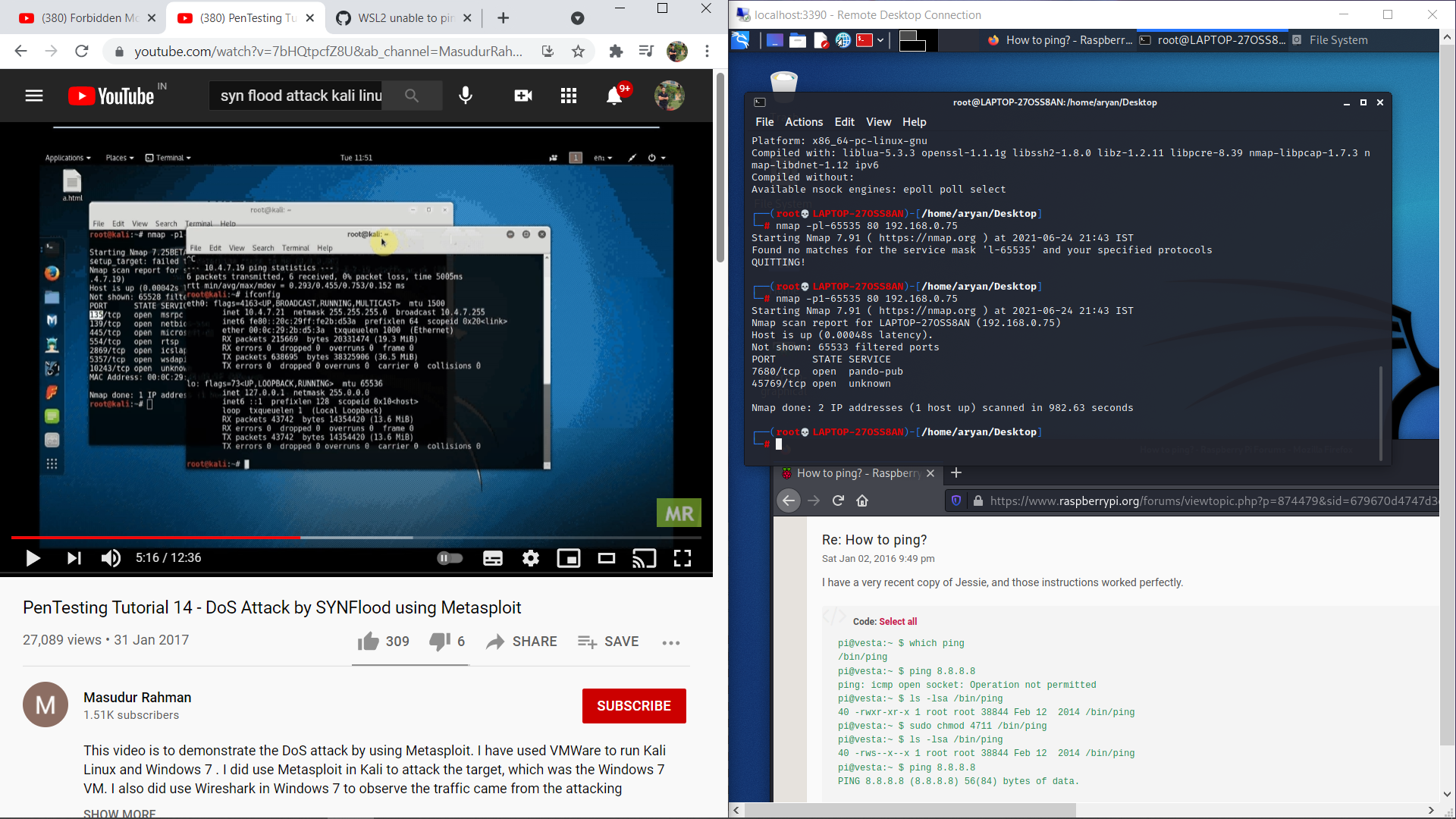


Fig. 9. Open ports

Now remember these ports and open metasploit and open synflood auxiliary and use that for exploitation by setting all the options see Fig. 10. And Fig. 11.

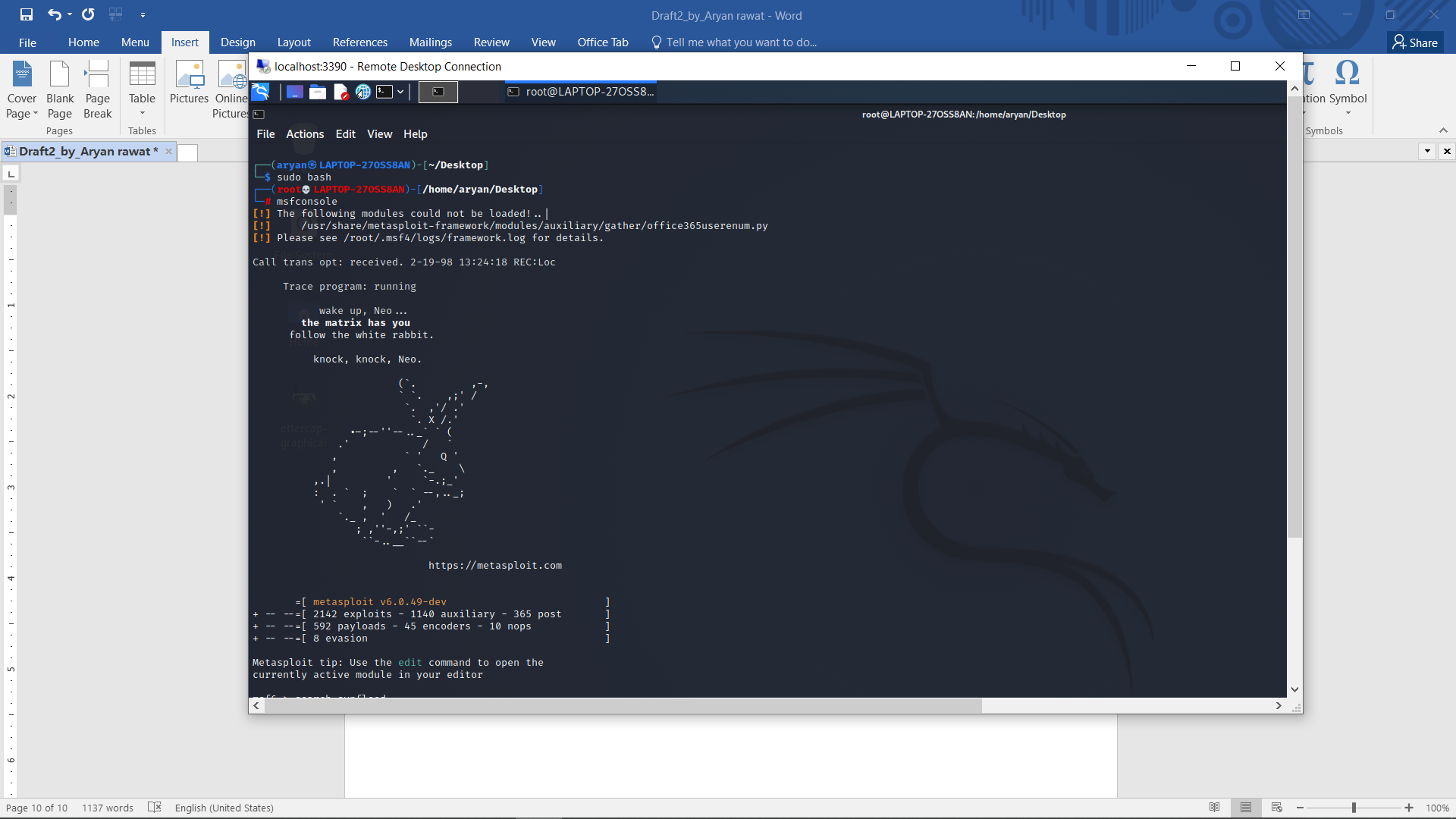


Fig. 10. metasploit

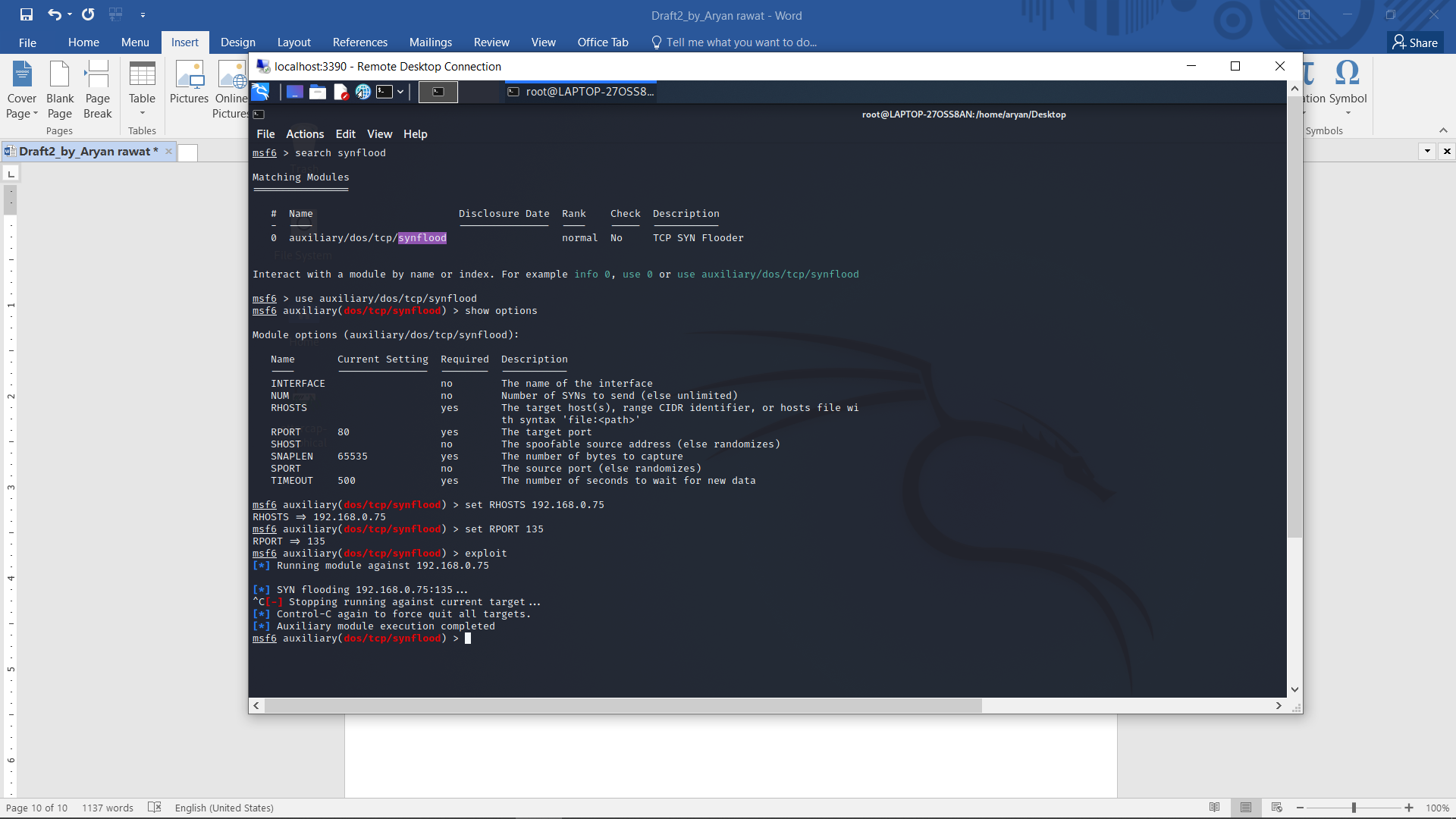


Fig. 11. metasploit options

6) Set all options according to your need if you do not set “NUM” unlimited numbers of packets will be sent to the “RPORT” you mention in the options. RHOSTS will contain targets IP address which we noted earlier.

Now run Wireshark in target machine and you can observe the synflood see Fig. 12. -a general Wireshark window looks like.

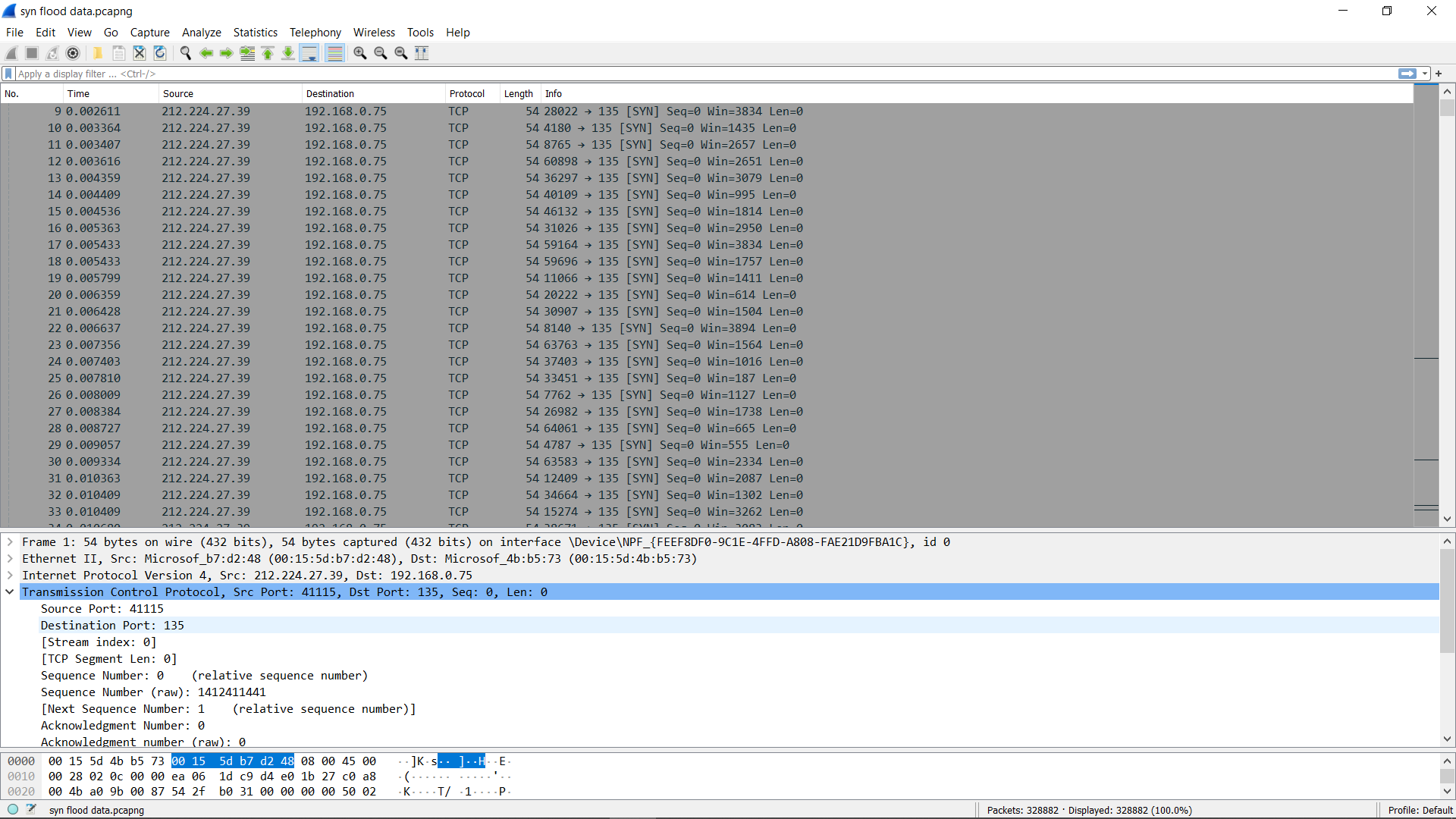


Fig. 12. SYN packets captured

Result: .Almost 30k packets were captured in Wireshark coming from the Linux system.

You can see before and after CPU utilization in snapshots below.

(Captured packets: <https://drive.google.com/file/d/1juBSpiNKSfBFVpW_iknI9He0hi2qV887/view?usp=sharing>). The target machine was overwhelmed by so many SYN packets and crashed eventually. See Fig. 13. And Fig. 14.

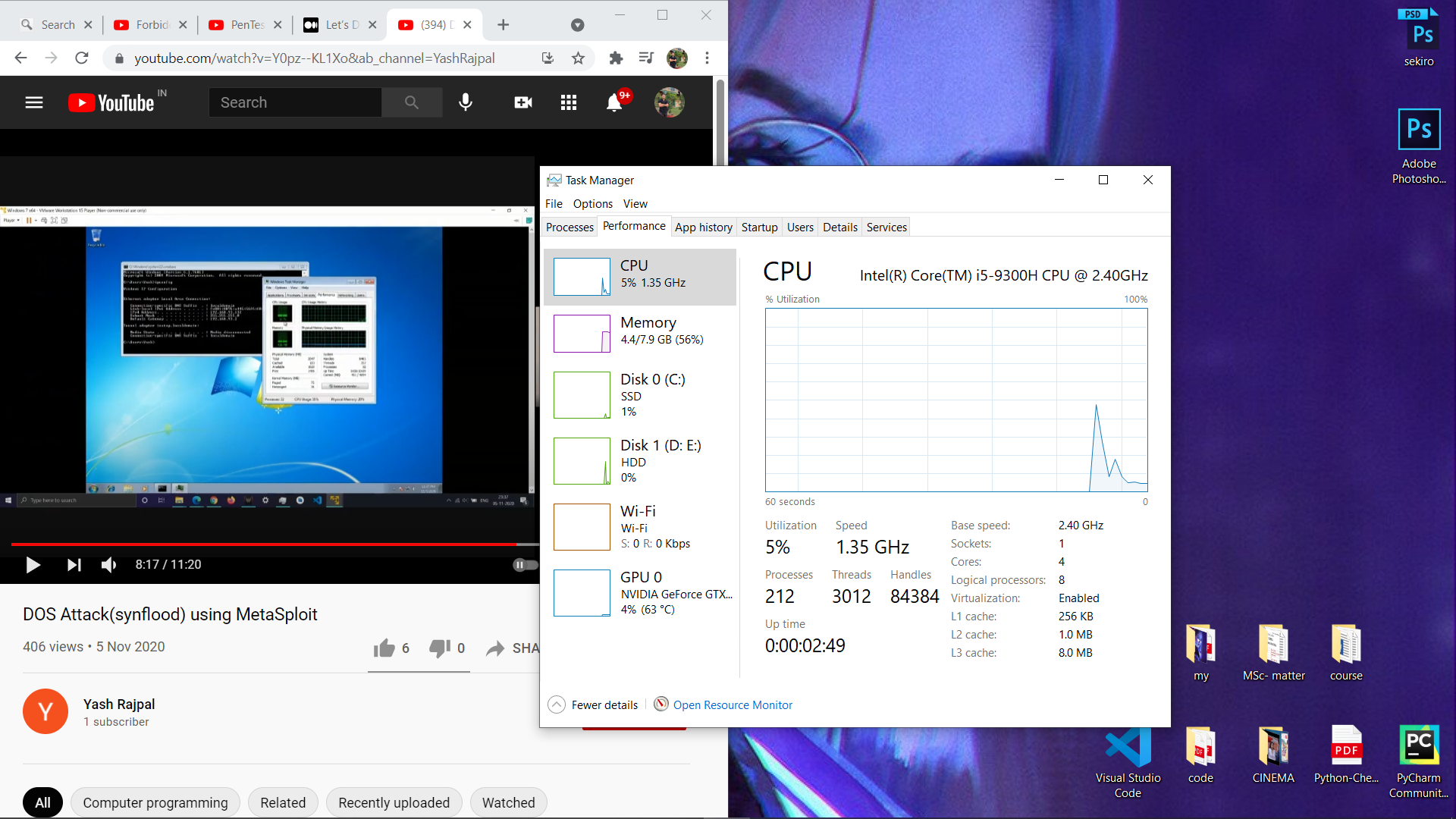


Fig. 13. Before SYN flood

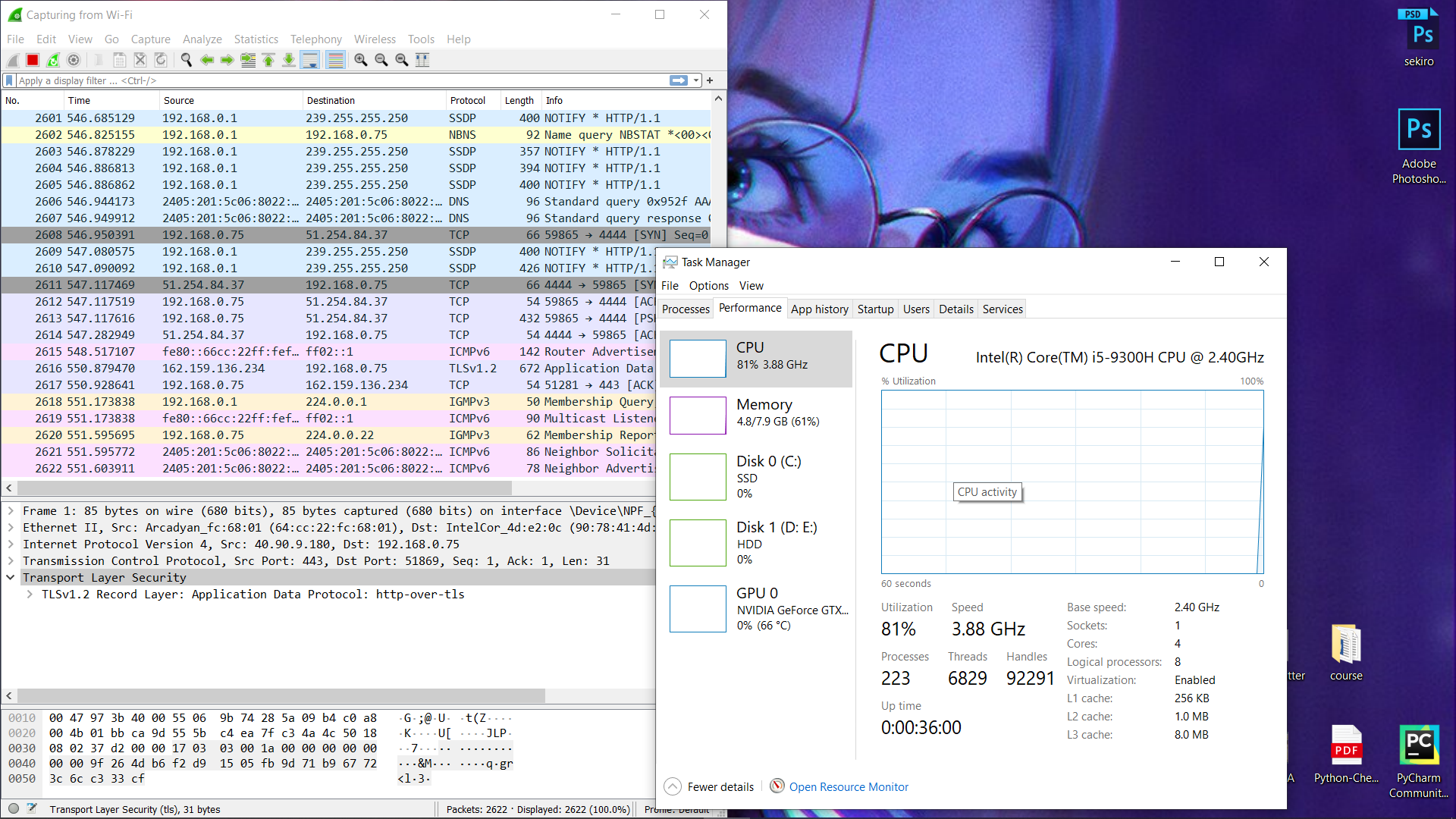


Fig. 14. After SYN flood

We can observe the following aspects and defend ourselves:

1) Target port

We can close the open target port by using windows firewall.

2) Senders IP

We can ban the senders IP from our LAN by using router gateway services or contacting ISP.

3) The source port.

4) Number of packets captured (bottom right) –packets captured more than usual amount can give us a clue about upcoming attack.

5) The type and info about packets in this case which are all SYN which gives us identifications about synflood. We can immediately seek help from ISP and resolve the issue.

6) Size of packets

7) We can install IPS (Intrusion Prevention System) and IDS (Intrusion detection system) to detect malicious traffic behavior.

8) Detection Using AI

Using neural network and fuzzy logics has been proved to be advantageous as much as the statistical approach when it comes to detect SYN flood attacks.

Fuzzy logic is a way of cognitive perceptive that acts just like human beings. Fuzzy logics shows judgement similar to humans and gives all in-between potentials among values Yes or No which is considered to be more precise, such as-

* surely yes
* maybe yes
* cannot say
* maybe no
* surely no

According to a model proposed by [41] represented in fig. 15. The first block consists of technique which classifies packets coming from the network traffic, here especially every header of packet is recorded to confirm if it’s TCP/SYN packet. If the recorded fragment offset value is zero in header then it’s considered a normal TCP packet whereas if the SYN flag in the TCP is 1 then it’s considered a SYN packet which is maybe attack. Then the packet classifier block forwards the packets to second part of system which is fuzzy logic system and this block is really responsible for detection of attack. This system is considered more accurate and highly responsive than the CUSUM (cumulative sum) algorithm.

Attack   
 possibility

Traffic

Packets

Classification

Fuzzy System

Fig. 15. Fuzzy logic System [41]

[42] Discussed the occurrence of DoS attack in actual period of time based on fuzzy logic. The method discussed was deeply observed and examined and according to method it has two mix methods:

1) Statistical examination of the network packets and time series to look out for statistical limitations that ends up from SYN floods.

2) Deducing the intensity of SYN flood using fuzzy logic.

This system was able to efficiently detect DDoS SYN floods.

Some limitations of this AI model was:

1) Small amount of attack SYN packets were missed during classifying the packets which can result in showing more false values.

2) System should be running prior to attacks to give accurate response time.

3) Small or light SYN floods are not detected promptly.[42]

# CONCLUSION

Next generation networks act as both boon and bane as they are now able to provide fast and convenient services but at the same time provide a platform to perform malicious activities like stealing personal data, shutting down servers, stealing identities and many more. While these situations are alarming they can be easily prevented by using proper tools and system. Having broad knowledge of NGN, knowing the working of next generation networks and security and privacy features of network also plays an important role in improving your security and privacy.

# REFERENCES

1. Kumar, S., Cengiz, K., Vimal, S. et al. Energy Efficient Resource Migration Based Load Balance Mechanism for High Traffic Applications IoT. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-021-08269-7.

2. Kumar, S., Ranjan, P., Ramaswami, R., & Tripathy, M. R., “Energy Efficient Multichannel MAC Protocol for High Traffic Applications in Heterogeneous Wireless Sensor Networks,” Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering , Vol. 10, No. 3, pp. 223-232, 2017.

3. A. Engelbrecht, Computational Intelligence: An Introduction, 2nd ed. New York, NY, USA: Wiley, 2007.

4. Kumar, S., Ranjan, P., Ramaswami, R., & Tripathy, M. R., “Resource efficient clustering and next hop knowledge based routing in multiple heterogeneous wireless sensor networks,” International Journal of Grid and High Performance Computing (IJGHPC) , Vol. 9, No. 2, pp. 1- 20, 2017.

5. Q. Lijun, Z. Jinkang, and S. Zhang, ‘‘Survey of wireless big data,’’ J. Commun. Inf. Netw., vol. 2, no. 1, pp. 1–18, 2017.

6. Punhani, A., Faujdar, N., Kumar, S., “Design and Evaluation of Cubic Torus Network-on-Chip Architecture” accepted and published by International Journal of Innovative Technology and Exploring Engineering (IJITEE) Volume-8 Issue-6, April 2019 ISSN: 2278-3075.

7. A. Zappone, M. Di Renzo, M. Debbah, T. T. Lam, and X. W. Qian, Model-aided wireless artificial intelligence: Embedding expert knowledge in deep neural networks for wireless system optimization, IEEE Vehicular Technol. Mag., vol. 14, no. 3, pp. 60–69, 2019.

8. Dubey, G., Kumar, S., Navaney, P. "Extended Opinion Lexicon and ML based Sentiment Analysis of tweets: A novel Approach towards Accurate Classifier", International Journal of Computational Vision and Robotics (IJCVR), Inderscience Publishers, 2020 , 10(6), pp. 505-521.

9. D. Naboulsi, M. Fiore, S. Ribot, and R. Stanica, Largescale mobile traffic analysis: A survey, IEEE Commun. Surv. Tutorials, vol. 18, no. 1, pp. 124–161, 2016

10. Sunil Kumar et al., “Evolution of Software-Defined Networking Foundations for IoT and 5G Mobile Networks” 2020/10, Pages 350, IGI Publisher, ISBN 9781799846857.

11. F. K. Jondral, ‘‘Software-defined radio-basics and evolution to cognitive radio,’’ EURASIP J. Wireless Commun. Netw., vol. 2005, no. 3, Dec. 2005, Art. no. 652784.

12. Kumar, S., Ranjan, P., Ramaswami, R., & Tripathy, M. R., “Energy aware distributed protocol for heterogeneous wireless sensor network” has been published by International Journal of control and automation, Vol.8, no. 10(2015), pp.421-430, http://dx.doi.org/10.14257/ijca.2015.8.10.38.

13. J. Mei, X. B. Wang, and K. Zheng, Intelligent network slicing for V2X services toward 5G, IEEE Netw., vol. 33, no. 6, pp. 196–204, 2019

14. Singh, P., Bansal, A., Kumar, S., “Performance analysis of various information platforms for recognizing the quality of Indian roads”, Proceedings of the Confluence 2020-10 th International Conference on Cloud Computing, Data Science and Engineering, 2020, pp. 63- 76, 9057829.

15. I. F. Akyildiz, P. Wang, and S.-C. Lin, ‘‘SoftAir: A software defined networking architecture for 5G wireless systems,’’ Comput. Netw., vol. 85, pp. 1–18, Jul. 2015.

16. Reghu, S., Kumar, S., “Development of Robust Infrastructure in Networking to Survive a Disaster”. 2019 4 th International Conference on Information Systems and Computer Networks, ISCON 2019, 2019, pp. 250-255, 9036244.

17. S. Dreiseitl, L. Ohno-Machado, Logistic regression and artificial neural network classification models: A methodology review 35 (5–6) (2002) 352–359.

18. Kumar, S., Ranjan, P., Ramaswami, R., & Tripathy, M. R., “An NS3 Implementation of physical layer based on 802.11 for utility maximization of WSN”, Proceedings - 2015 International Conference on Computational Intelligence and Communication Networks, CICN 2015 , 2016, pp. 79-84 , 7546060.

19. Mathworks. Matlab neural network toolbox. https://uk.mathworks.com/p roducts/neural-network.html, 2016.

20. Kumar, S., Ranjan, P., Ramaswami, R., & Tripathy, M. R., “A Utility Maximization Approach to MAC Layer Channel Access and Forwarding”, Progress in Electromagnetics Research Symposium , 2015 , 2015-January, pp. 2363-2367.

21. F. Boccardi, R. W. Heath, Jr., A. Lozano, T. L. Marzetta, and P. Popovski, ‘‘Five disruptive technology directions for 5G,’’ IEEE Commun. Mag., vol. 52, no. 2, pp. 74–80, Feb. 2014.

22. Kumar, S., Ranjan, P., Ramaswami, R., & Tripathy, M. R., “EMEEDP: Enhanced multi-hop energy efficient distributed protocol for heterogeneous wireless sensor network” Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015 , 2015, pp. 194-200.

23. E. C. Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Ktenas, N. Cassiau, L. Maret, and C. Dehos, 6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication, IEEE Vehicular Technol. Mag., vol. 14, no. 3, pp. 42–50, 2019.

24. Kumar, S., Ranjan, P., Ramaswami, R., “Energy optimization in distributed localized wireless sensor networks”, Proceedings of the International Conference on Issues and Challanges Intelligent Computing Technique (ICICT), DOI: 10.1109/ICICICT.2044.678130.

25. Philip Russom, “Big Data Analytics” Tdwi Research, Fourth Quarter 2011, pp. 5–11.

26. Builtin.com, “Artificial Intelligence, What is Artificial Intelligence? How does it work?”, available at : https://builtin.com/artificial-intelligence

27. Certes.co.uk, “Types of Artificial Intelligence: A Detailed Guide”, 20thdecember 2018, available at : https://certes.co.uk/types-of-artificial-intelligence-a-detailed-guide

28. M. Singh and G. Baranwal, “Quality of Service (QoS) in Internet of Things,” 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, pp. 1-6, doi: 10.1109/IoT-SIU.2018.8519862.

29. Sunil Kumar, “Advantages and Disadvantages of Artificial Intelligence”Towards data science, 25, Nov.2019, available at: https://towardsdatascience.com/advantages-and-disadvantages-of-artificial-intelligence-182a5ef6588c

30. GeeksforGeeks, “TCP 3-Way Handshake Process”, 06th September 2019, available at : https://www.geeksforgeeks.org/tcp-3-way-handshake-process

31. Builtin.com,“What Is Throughput in Networking? Bandwidth Explained”, 19th September 2019, Available at: https://www.dnsstuff.com/network-throughput-bandwidth

32. wireshark.org, “TCP Analysis”, available at :https://www.wireshark.org/docs/wsug\_html\_chunked/ChAdvTCPAnalysis.html

33. Amazon Cloud Foundation, “Cloud Concepts Overview”, Module 1, © 2018 Amazon Services, Inc. or its affiliates. All rights reserved

34. F. K. Jondral, ‘‘Software-defined radio-basics and evolution to cognitive radio,’’ EURASIP J. Wireless Commun. Netw., vol. 2005, no. 3, Dec. 2005, Art. no. 652784.

35. https://www.itu.int/en/ITU-T/studygroups/2013-2016/Pages/default.aspx

36. Anusha G E, 2013, Security Challenges for Next Generation Networks, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCRTICE – 2013 (Volume 1 – Issue 04),

37. https://www.cloudflare.com/ddos/

38. https://www.geeksforgeeks.org/next-generation-network-ngn/

39. http://hdl.handle.net/10603/286568

40. https://blog.securityonion.net/

41. T. Tuncer and Y. Tatar, "Detection SYN Flooding Attacks Using Fuzzy Logic," in International Conference on Information Security and Assurance, 2008, pp. 321-325.

42. . Z. Xia, Lu, S., Li, J., & Tang, J., "Enhancing DDoS Flood Attack Detection via Intelligent Fuzzy Logic," Informatica (Slovenia), pp. 497-507, 2010.