Detecting and Blocking Encrypted Anonymous Traffic using Deep Packet Inspection

Parita Chandrakant Parekh[1], Prof. Jayshree Upadhyay [2]

[1] *PG Scholar, ITSNS, GTU PG SCHOOL, Gujarat, India*
[2] *Assistant Professor, CSE, ASOIT, Gujarat, India*

ABSTRACT

Internet is vital source for gathering information and main concern is to improve Security. With rapid growth in several types of attacks, many protection mechanism has took place to improve the privacy and security of sensitive information for Users. The major concern lies in the network is lots of suspicious activity took place in it. One of the widely used technique Intrusion detection system which helps to identify the intrusion, abnormal, unknown activity inside the network. To counter these problems a new approach is needed .Tor traffic is one of the major problem as it provides anonymity to the user and hard to detect and it is a threat to the organization. A new system is proposed which analyze suspicious threat inside the network. Based on the analysis, further perform the deep packet inspection to make sure that threat is really doing suspicious activity in background. After identifying that threat, system will block it from the network so that it will no longer be part of it.

Keyword: - *DPI, IDS2, TOR, and threat*

1. INTRODUCTION

Networking can be defined as the interconnection of the multiple devices, termed as nodes connected with multiple paths for sending and receiving the data. There are multiples devices i.e. (Router, Switch, bridge) connected for the purpose of communication between sender and receiver inside the network [1].
Ability to share resources can be printers, scanners, files, any much more that helps transfer any resources within seconds able to transfer the data easily.

1.1 Introduction to DPI

It is type of data processing of data sent across the network packets. There are multiple headers for the IP packets, in that first phase (IP header format) header of IP packets and the second header (TCP, UDP) is considered as to be shallow inspection of the packet. Making sure that the data carries the right format or contains malicious source, virus and many more
To acquire more information regarding the packets using deep packet inspection by applying port mirroring. To enable advanced network management, user services and security related function. DPI is used for the wide range of the application. [3]

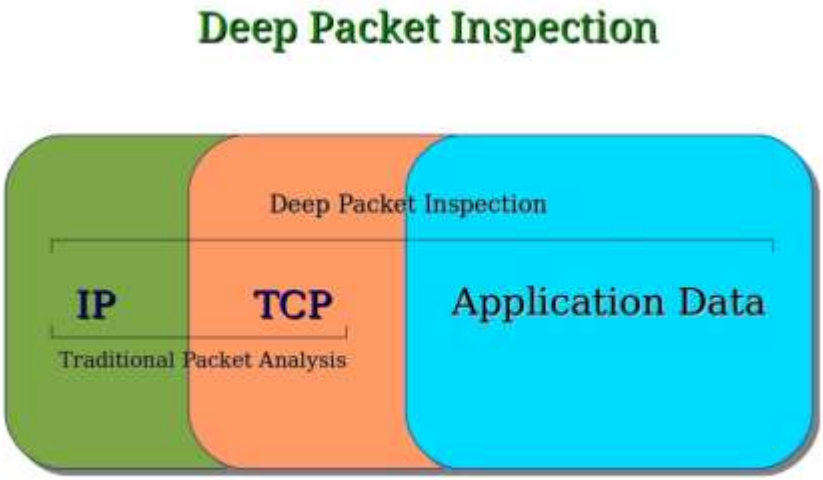

Fig -1: Deep Packet Inspection

1.2 Application of DPI Technology

Deep Packet Inspection has several application some of them are listed below:

- Network Security
- Anti-Malware
- URL- Filtering
- Protocol and application Recognition
- Network Management
- Billing and Metering of traffic

2. OVERVIEW

The system which is being implemented here needs an IDS to detect the malicious network so for that purpose we are using MALTRAIL. For capturing the packets we need Wireshark so that we can analyze them. The Deep Packet Inspection is important part of our proposed system so to perform that we will use nDPI. The blocking of malicious traffic is necessary part of the system, here we will use IPTABLES for that.

2.1 MALTRAIL

MALTRAIL is basically traffic detection system. This detection system mainly consist of four components.

- Traffic
- Sensor
- Server
- Client

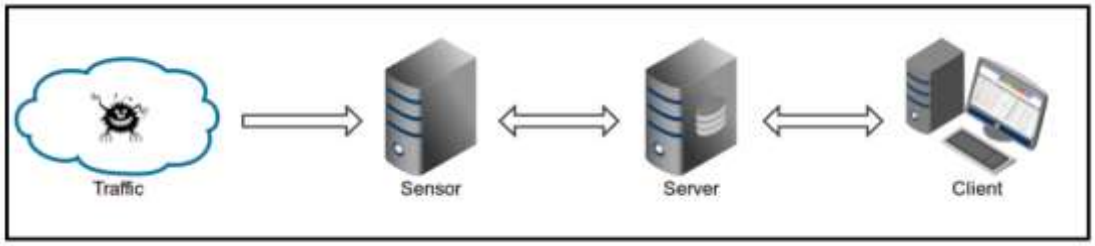

Fig -2: Architecture of MALTRAIL

2.2 Anonymous-Browser (TOR/Onion Router)

TOR is most prominent and famous tools for Internet Privacy and Anonymity service. Which means it is widely used service for anonymously accessing the internet, is made up of over-relay network, anonymous TCP-based application. It is able to one circuit for many TCP streams. Traffic passes with the fixed-size cell of 512 bytes with header and payload to it.

While surfing the internet there are various Flash objects, add-ons in regular internet but in TOR browser such attempts may disrupt the system or reveal logical address of the user. Anonymous browser uses exit relays to hide the user's traffic. It is vulnerable to many passive and active attacks within the network. It is meant to communicate with the relays

As per the work, TOR is used as browser for anonymous service. While surfing through the anonymous platform, it may or may not be safe. So the system which analyze the traffic generated by the TOR browser and finds the information from the traffic.

2.3 WIRESHARK (Packet Analyzer)

WIRESHARK is one of the open-source tool for examine the network packets. It is one of the network packet analyzer for the Network Administrator, Security engineers, Forensics experts, etc. It is used to examine the network traffic from the captured packets and tries to display the details information of the packets. There are many features of Wireshark mention below:

- Supports both Windows as well as Linux platforms
- Capture live packet from network interface.
- Files containing captured packet with tcpdump/windump.
- Filters the packets as per the criteria.
- Colorize packet displayed based on the applied filters to it.
- Create various statistics of the captured packets.

2.4 Deep Packet Inspection

Deep packet inspection (DPI) is used to analyze the in-depth of the packets sent over the Internet.DPI bring he analysis of the content of the packet into the picture which used for the several purpose like Identifying the Malicious Packets, Intrusion, and many more for various types traffic management. It allows to inspect the packet beyond the header and the footer of the packets content in-depth.DPI strips down the header and footer from the packet and inspect the payload.
As per the work DPI is to find the malicious, suspicious packets inside the network. To identify the packets in-depth and finds that any back-end suspicious activity signatures using DPI, able to get the detail information of the packets. It helps to monitor the traffic and keep away from the suspicious activity running, unknowingly from authorized person.

Main purpose to avoid the malicious content, injected to the websites, also to save from attackers. Using DPI the effectiveness and efficiency of the organization increases. nDPI is popular maintained OpenDPI library. It supports both Windows and Linux platform. nDPI.
It is suitable for traffic monitoring applications for the detection of the application-layer protocols. It supports the detection of the known protocols on non-standard ports.

2.5 IP Tables/NetFilters

Netfilter is a packet filtering utility for the linux-based versions. Iptables uses tables to organize its rules. In figure below the Iptable is depicted. Filter concerns about the filtering rule (Accept, Refuse, Ignore) the packets.

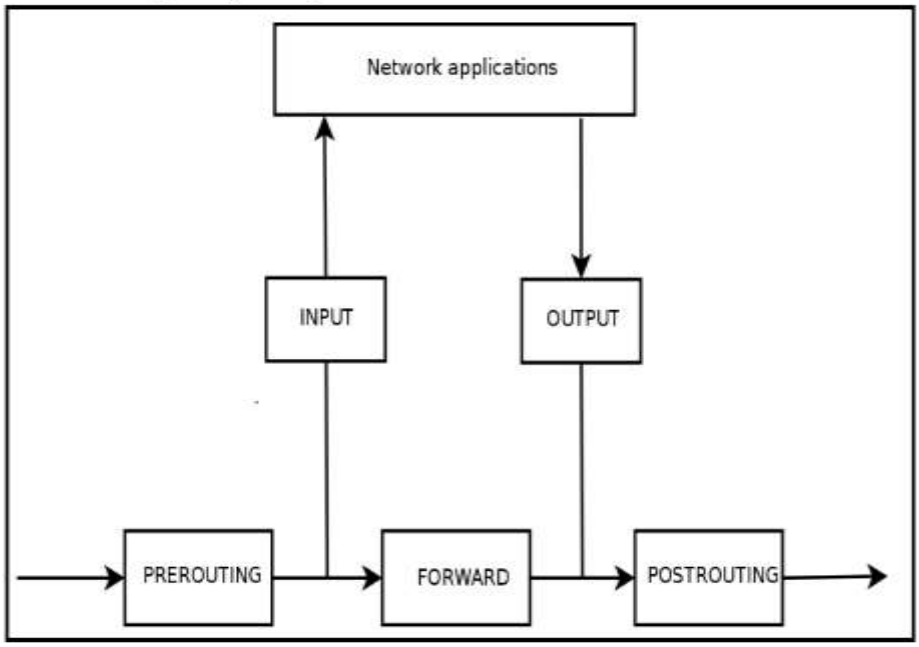

Fig -3: IPTABLES/NETFILTER ARCHITECTURE

3. PROPOSED SYSTEM

The Proposed system is design for detecting and blocking the suspicious traffic from the network. This system captures packets from the network, after that it performs Intrusion detection based on the packets captured. After that it checks whether the captured packet is found any threat is detected, if so then further inspect the packet deeply. During the inspection of the packet some characteristics of the suspicious activity is found then block the Packet. In this case system block afterwards it will not be part of it.

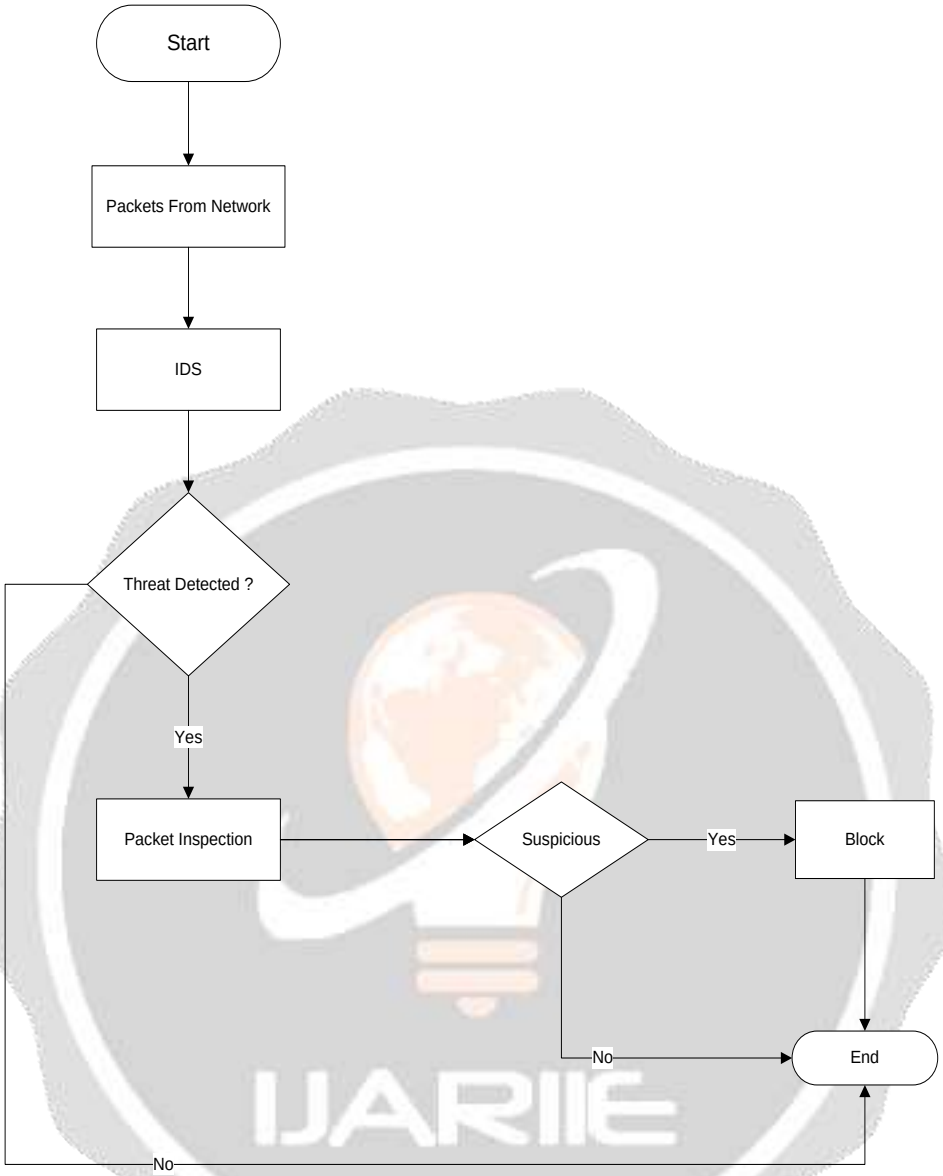

Fig -4: Flowchart of proposed system

As mentioned, that system consist of two main parts: Detection Part and Inspection Part. In detection part, if the malicious packets are generated then detection system any suspicious activity is not detected, then it will drop the packet. If found some intrusion then further analyze, based on the packet inspection.
According to the flow of the proposed system to identify the undetectable activity, identifies that the packet is malicious in intent. Further it will block by the system by applying some filters to it so that it will no longer be part of the above system.

4. IMPLEMENTATION

Pcapy is a Python extension module that enables software written in Python to access the routines from the pcap packet capture library.

Step 1 : Install pcapy using command ***sudo apt-get install git python-pcapy***

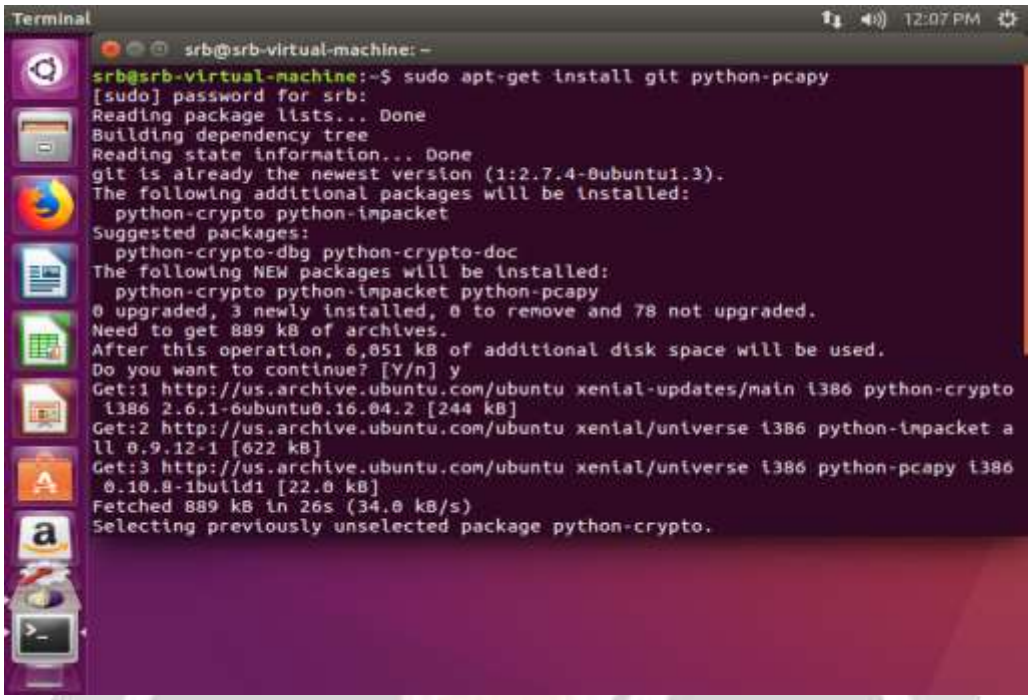

Fig -5: Installation of pcapy

Step 2 : Git clone the mailtrail using git clone https://github.com/stamparm/maltrail.git

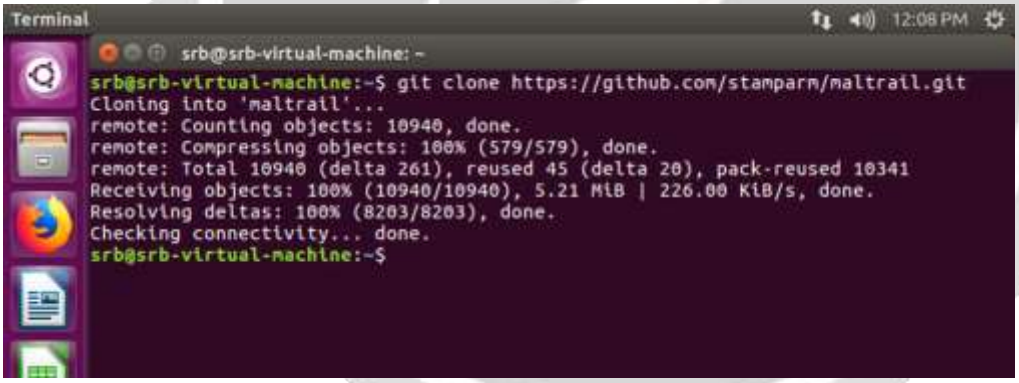

Fig -6: Installation of Maltrail

Step 3 : Start the maltrail sensor so that it can scan the network traffic by using command sudo python sensor.py

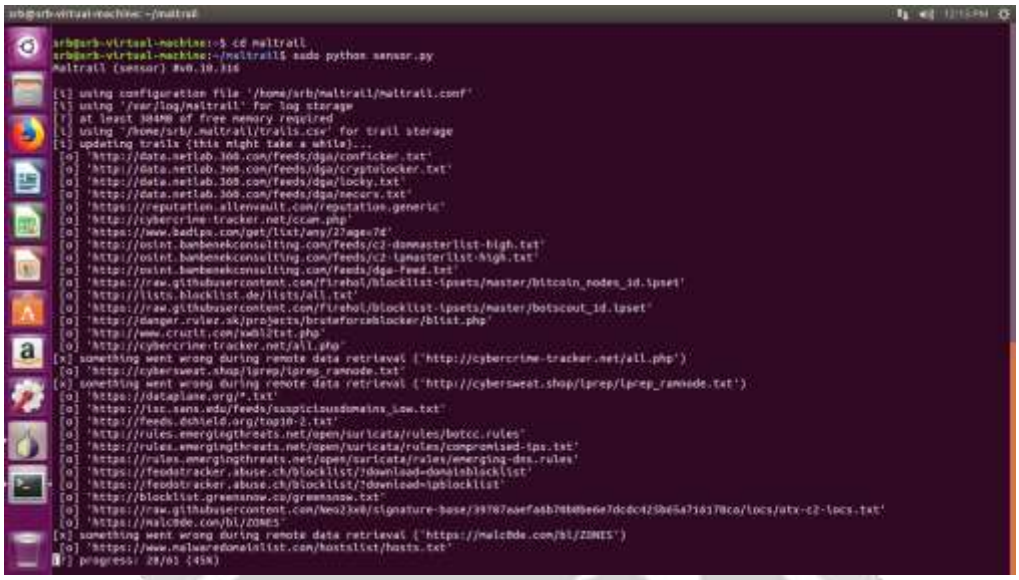

Fig -7: Starting of Maltrail sensor

Sensor(s) is a standalone component running on the monitoring node (e.g. Linux platform connected passively to the SPAN/mirroring port or transparently inline on a Linux bridge) or at the standalone machine (e.g. Honeypot) where it "monitors" the passing Traffic for blacklisted items/trails (i.e. domain names, URLs and/or IPs)

Step 4 : Search the desired page in TOR Browser ,our case it is www.wikipedia.org/wikimain_Page

Fig -8: Search wikipedia

Step 5 : Now open the maltrail directory using cd maltrail and Start the server using command pythonserver.py

Fig -9: Start Maltrail server

Step 6 : Open the wireshark and start capturing the live traffic

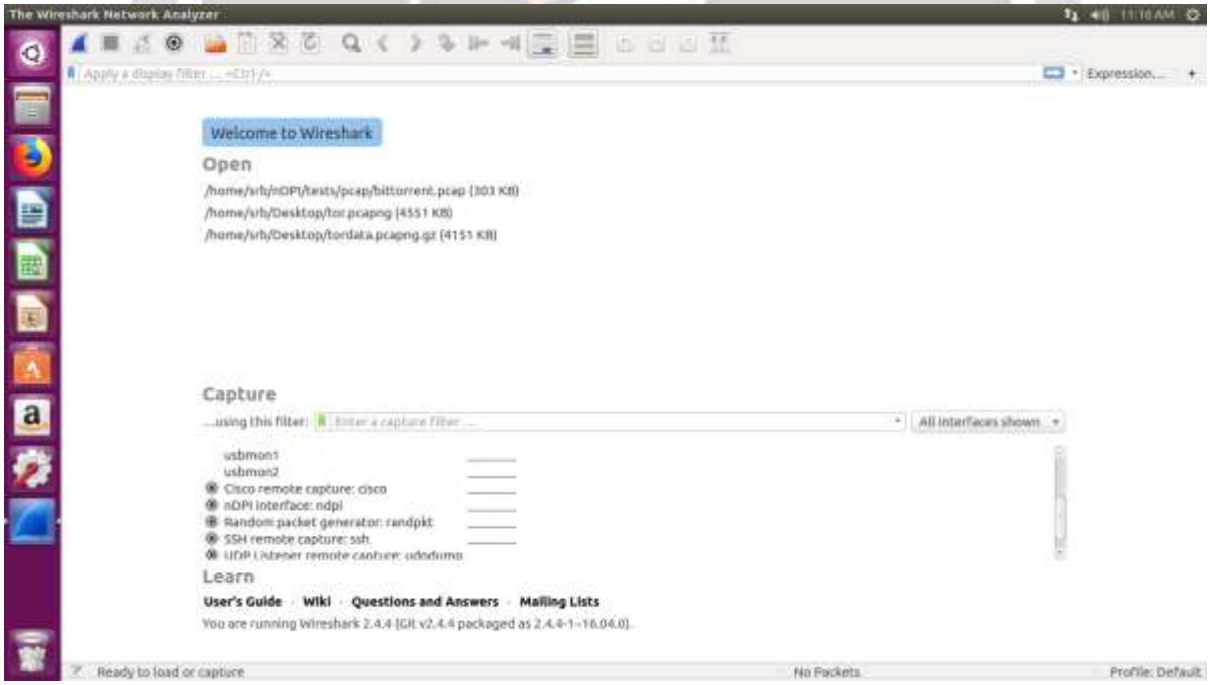

Fig -10: Launching Wireshark to capture packets

Step 7 : PING the malicious SINKHOLE attack ip using command ping –c 136.161.101.53
Ping the TOR IP using command ping –c 62.210.217.207 for scanning

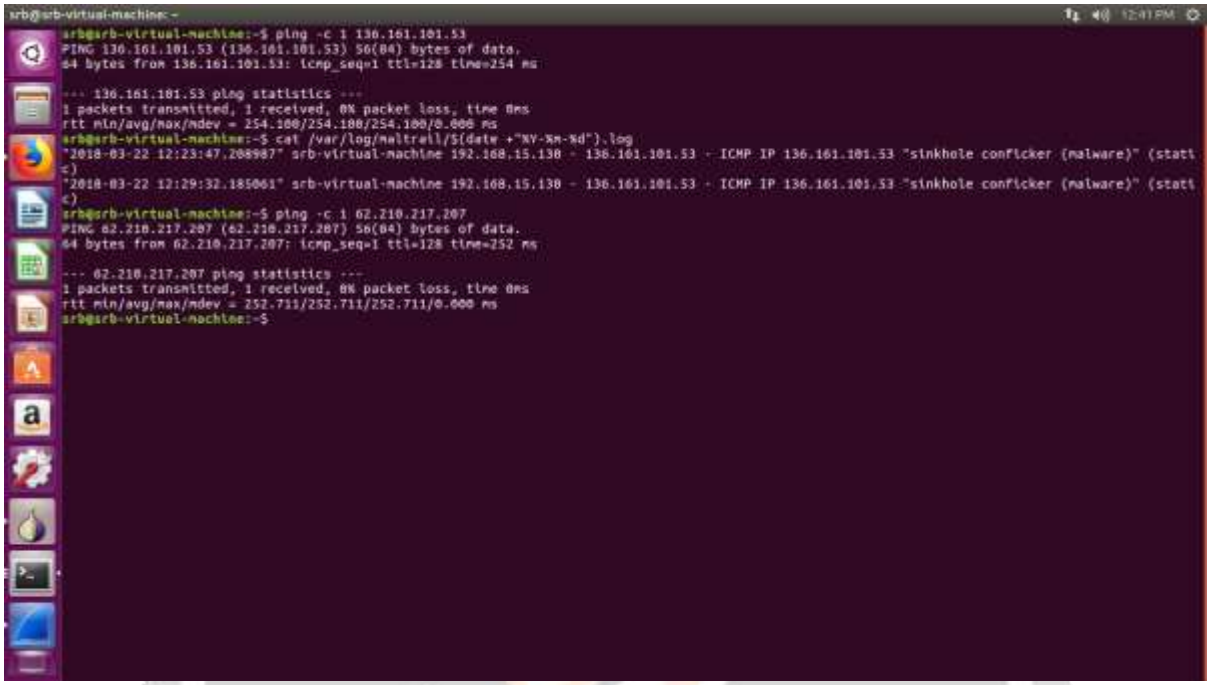

Fig -11: Pinging TOR IP and Malware

Here in the info section we can see TOR exit node and SINKHOLE CONFLIKER malware

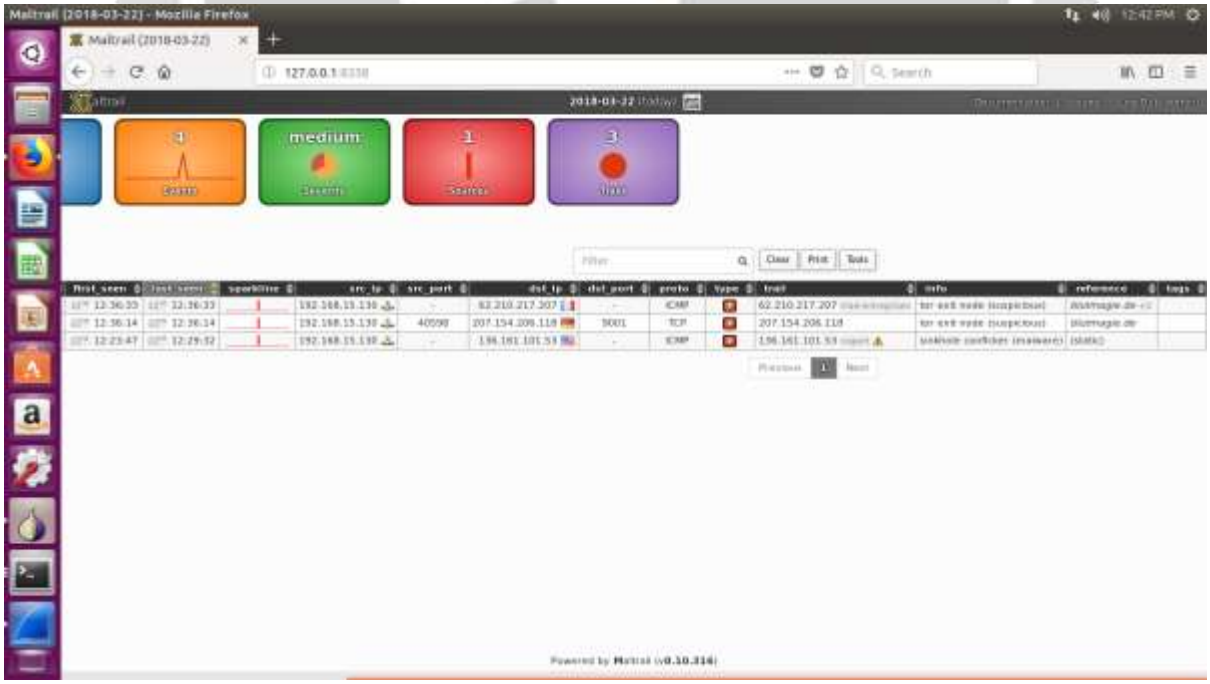

Fig -12: Maltrail panel

Step 8 **:** Inspecting packets we can see there is an encryption alert TLSv1.2 which is unusual

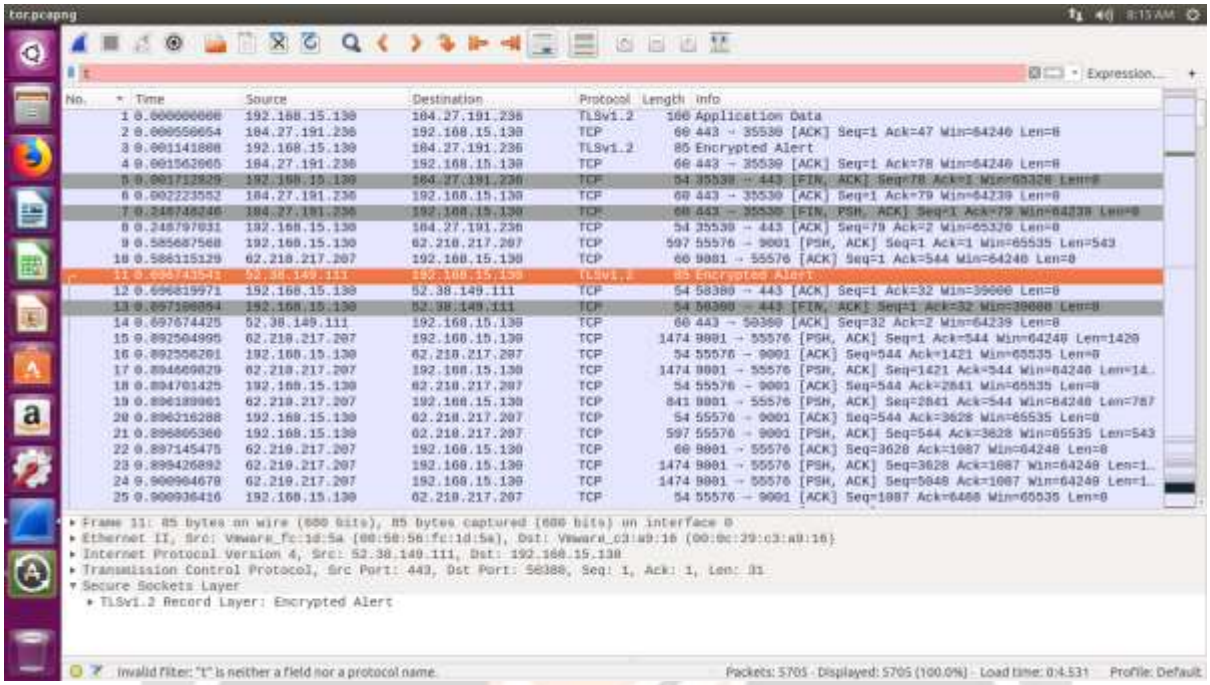

Fig -13: Inspecting packets searching for TLSv1.2

Step 9 : We will perform deep packet inspection using nDPI open library

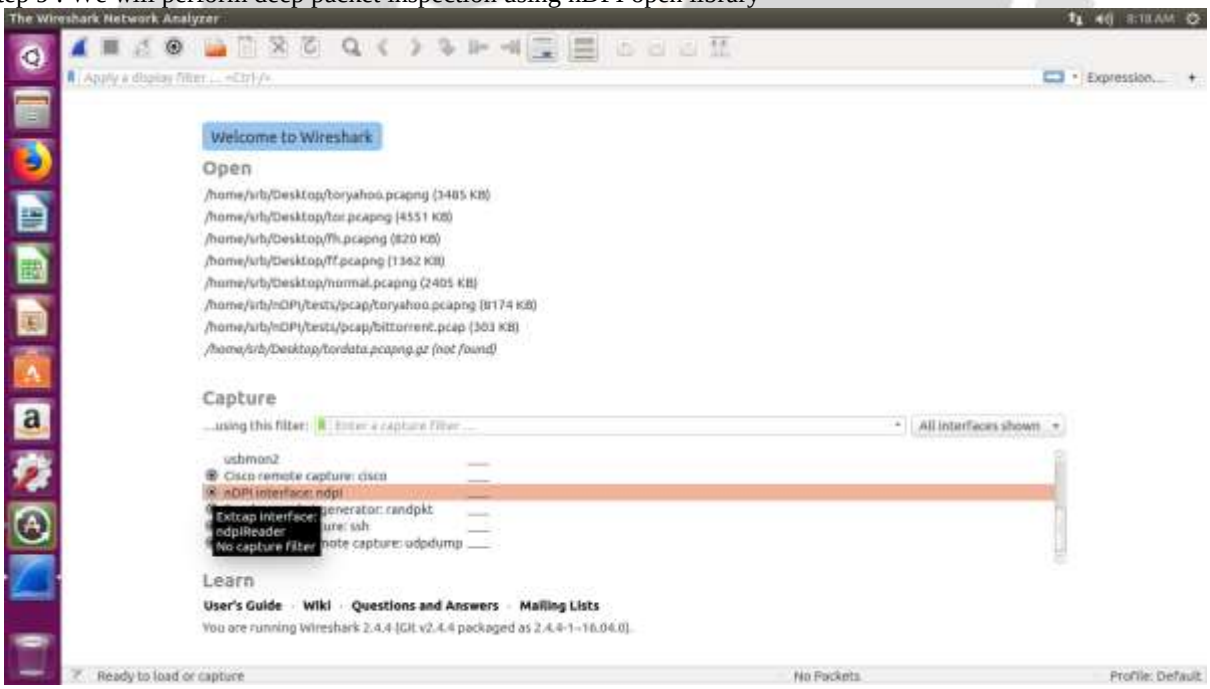

Fig -14: Perform DPI using nDPI

Step 10 : For destination ip 62.210.217.207 we can see TOR in protocol

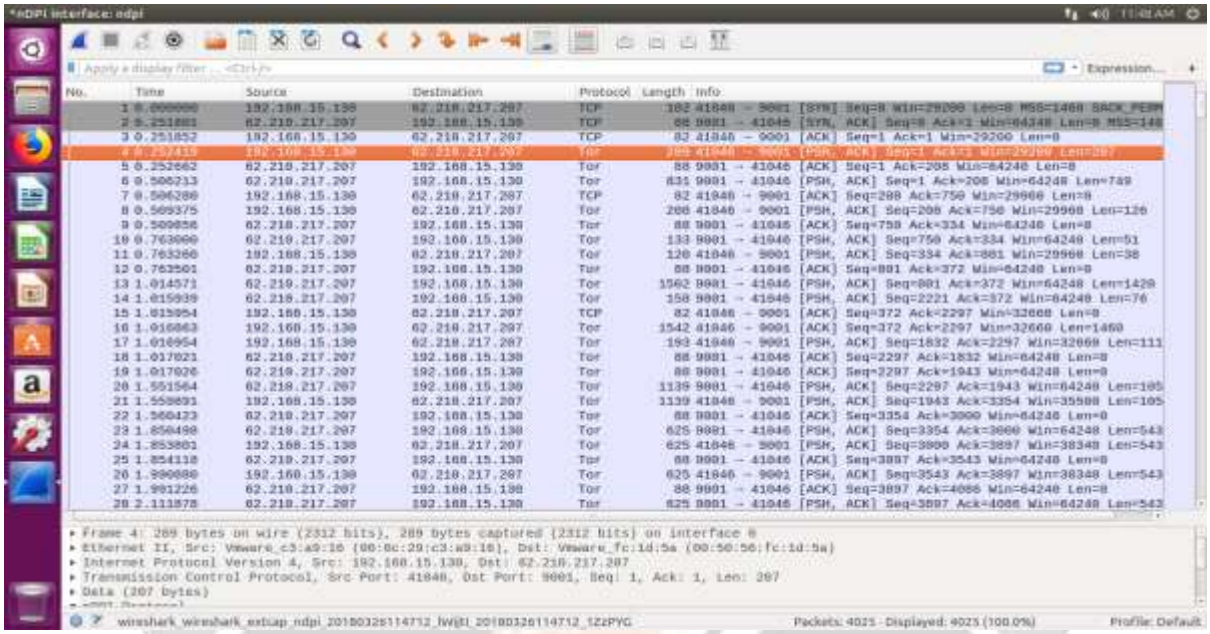

Fig -15: Deep Packet Inspection showing TOR IP's

Step 11 : The breakdown shows data which is attached in TCP [Protocols in frame: eth:ethertype:ip:tcp:data]

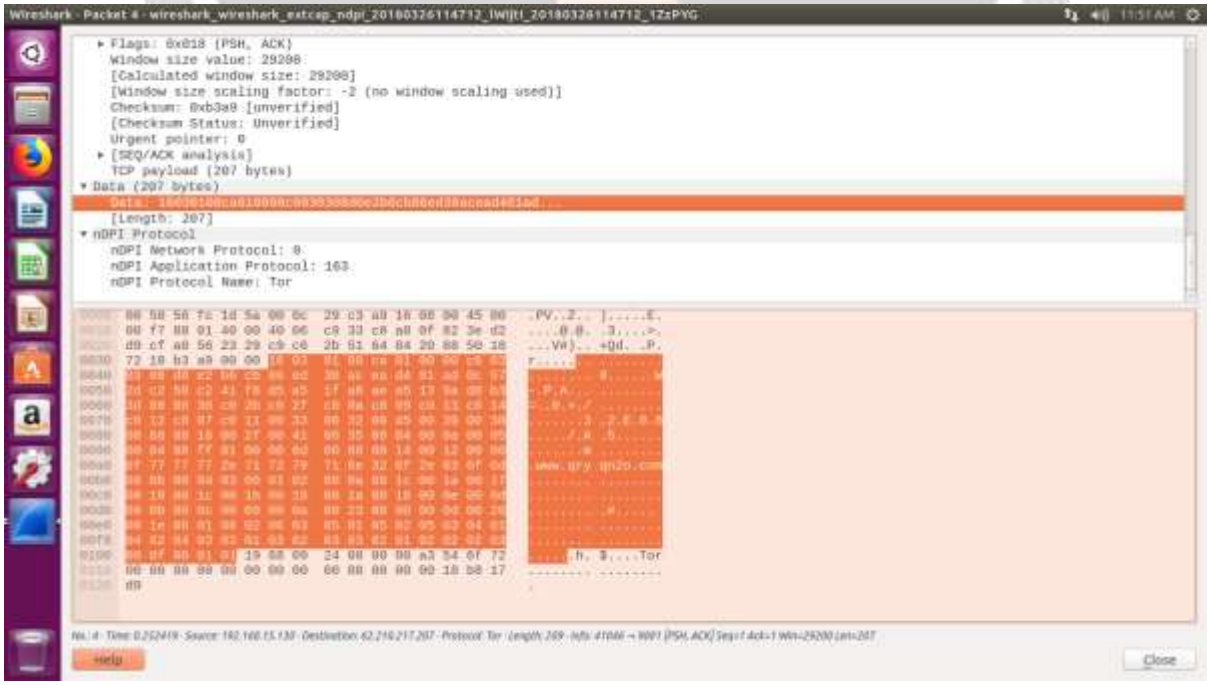

Fig -16: Breakdown of TCP [Protocols in frame: eth:ethertype:ip:tcp:data]

Step 12 : Breakdown of Tor frame [Protocols in frame: eth:ethertype:ip:tcp:data]

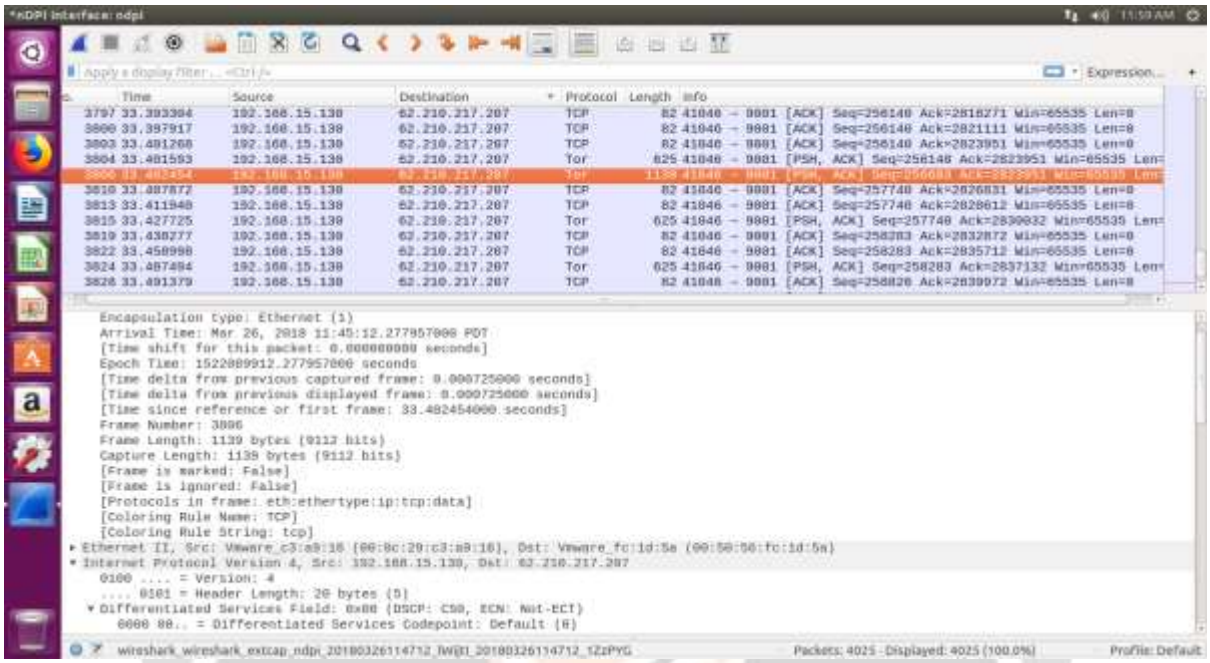

Fig -17: F Breakdown of TOR [Protocols in frame: eth:ethertype:ip:tcp]

As shown in figure the format for Tor frame is [Protocols in frame: eth:ethertype:ip:tcp:data] where data is suspiciously attached as the frame in normal packet shows itself as TCP but in Deep Packet Inspection we find that it is not TCP and originally it is TOR

Step 13 **:** Breakdown of TCP frame [Protocols in frame: eth:ethertype:ip:tcp]

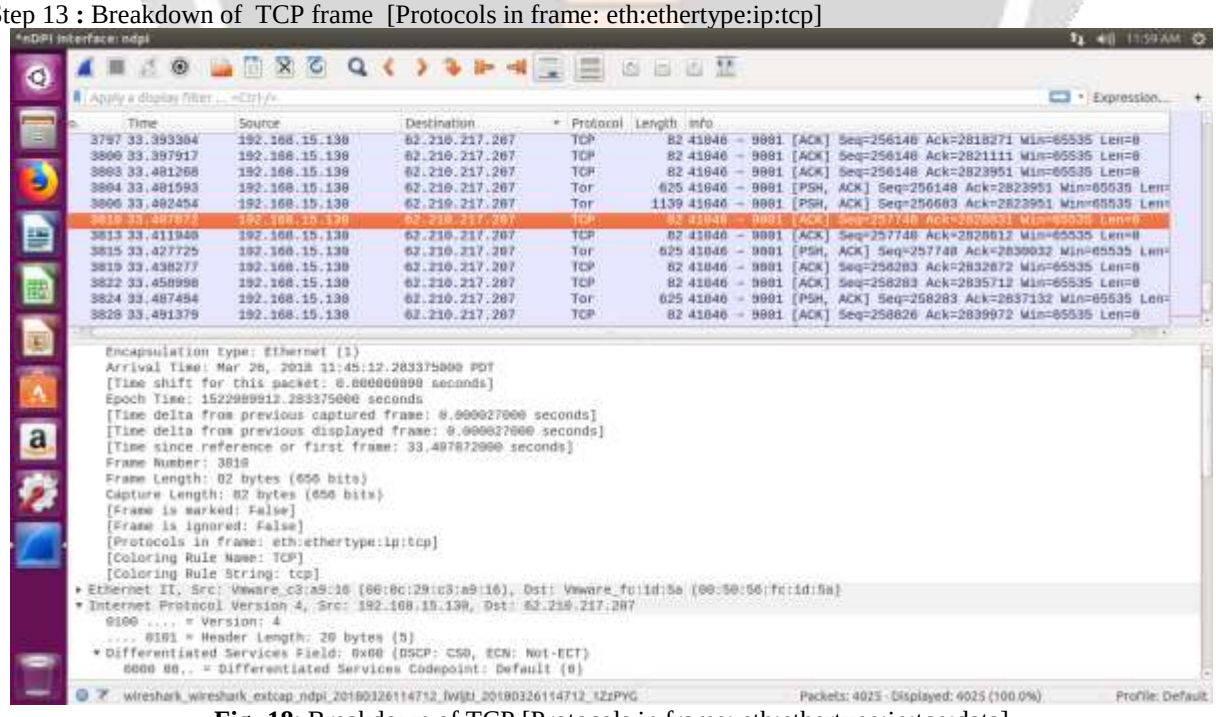

Fig -18: Breakdown of TCP [Protocols in frame: eth:ethertype:ip:tcp:data]

As shown in figure the format for TCP frame is [Protocols in frame: eth:ethertype:ip:tcp]

Step 14 : The nDPI Protocol statistics

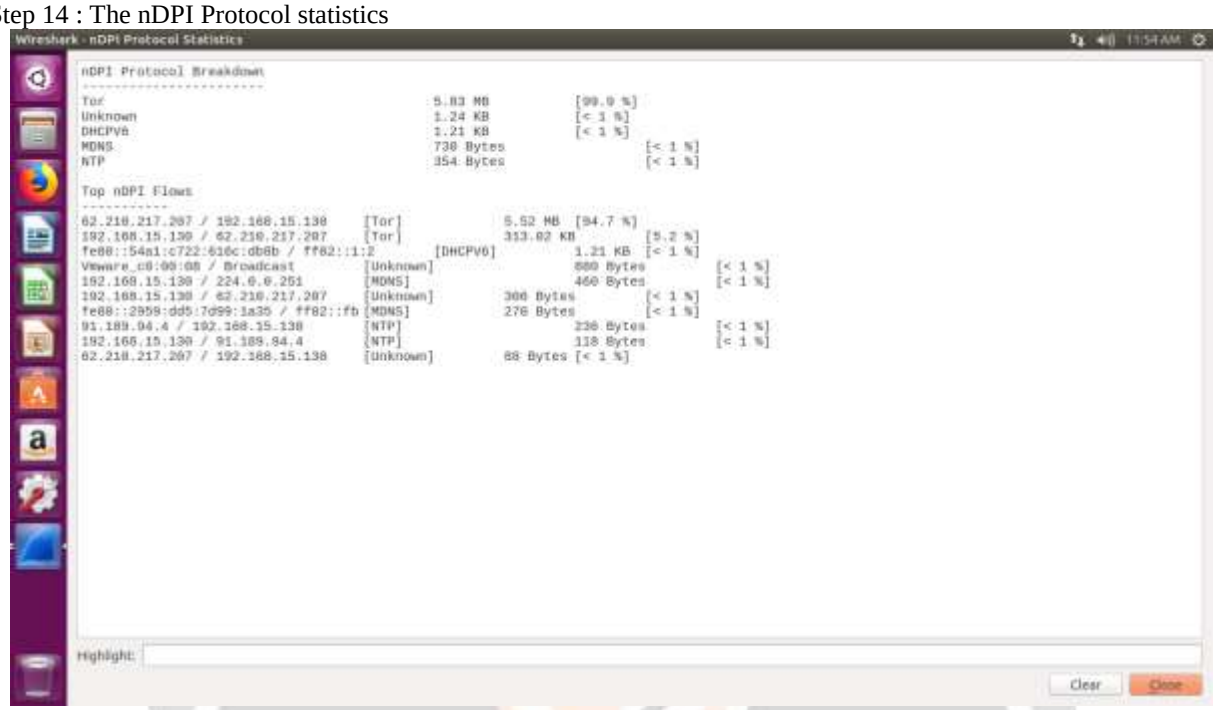

Fig -19: nDPI Protocol statistics

The nDPI Protocol Breakdown shows the presence of TOR TRAFFIC
Top nDPI Flows shows 62.210.217.207 / 192.168.15.130 as TOR and other which is its relay as 192.168.15.130 /62.210.217.207 as TOR flow.

Step 15: Opening Wireshark and find TOR IP which we found through Deep Packet Inspection, in this case it is 62.210.217.207

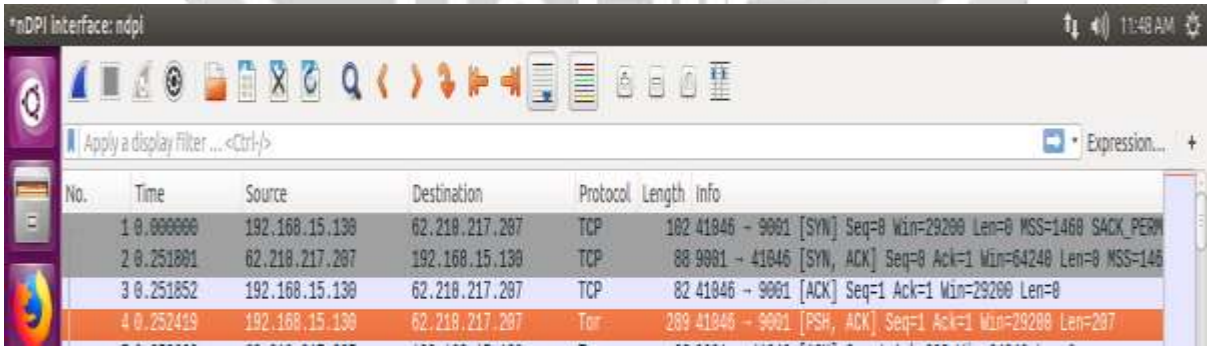

Fig -20: Identifying TOR IP using nDPI in Wireshark

Step 16: Block the IP through IP TABLES using command *sudo iptables –A INPUT –s 62.210.217.207 –j DROP*

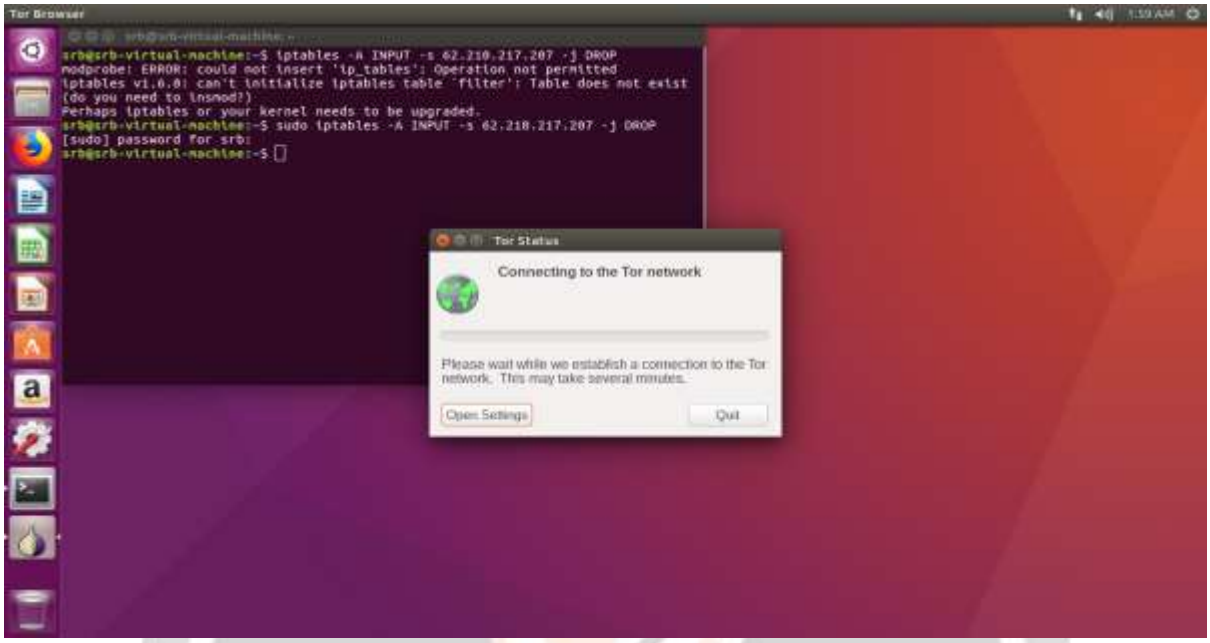

Fig -21: Blocking TOR IP using iptables

Step 17: Reopen TOR it will try to establish the connection with TOR Network

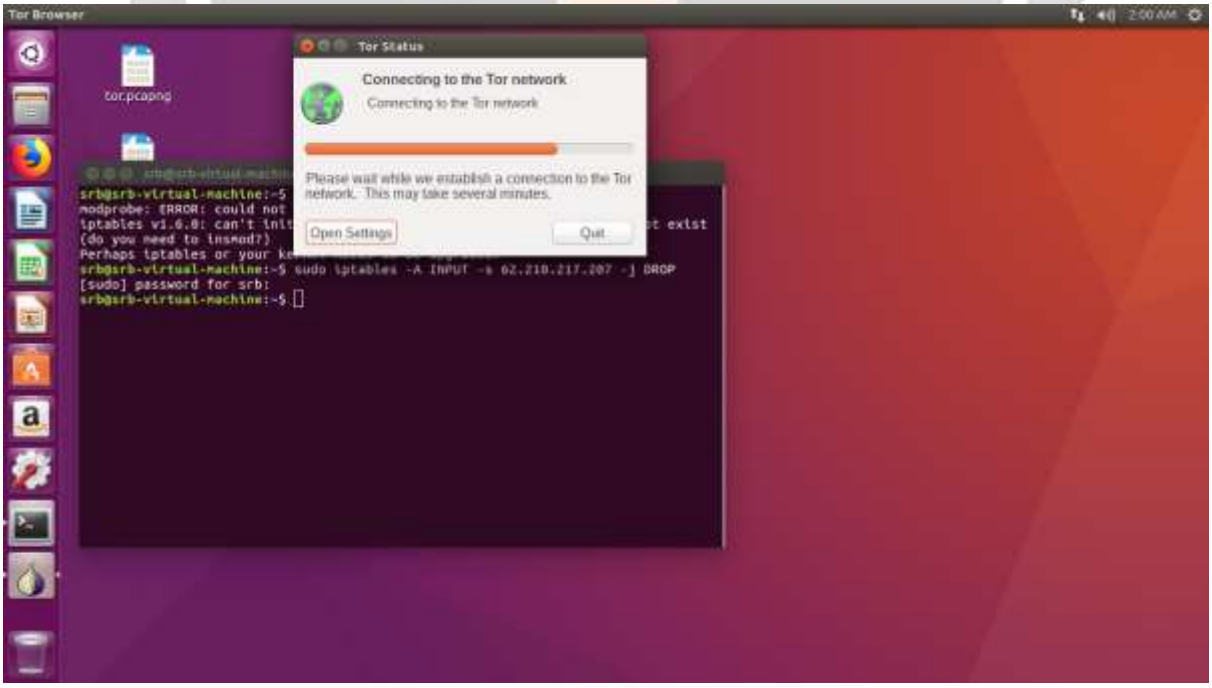

Fig -22: TOR trying to establish connection

Step 18: After blocking the TOR EXIT NODE it will refuse the connection with network

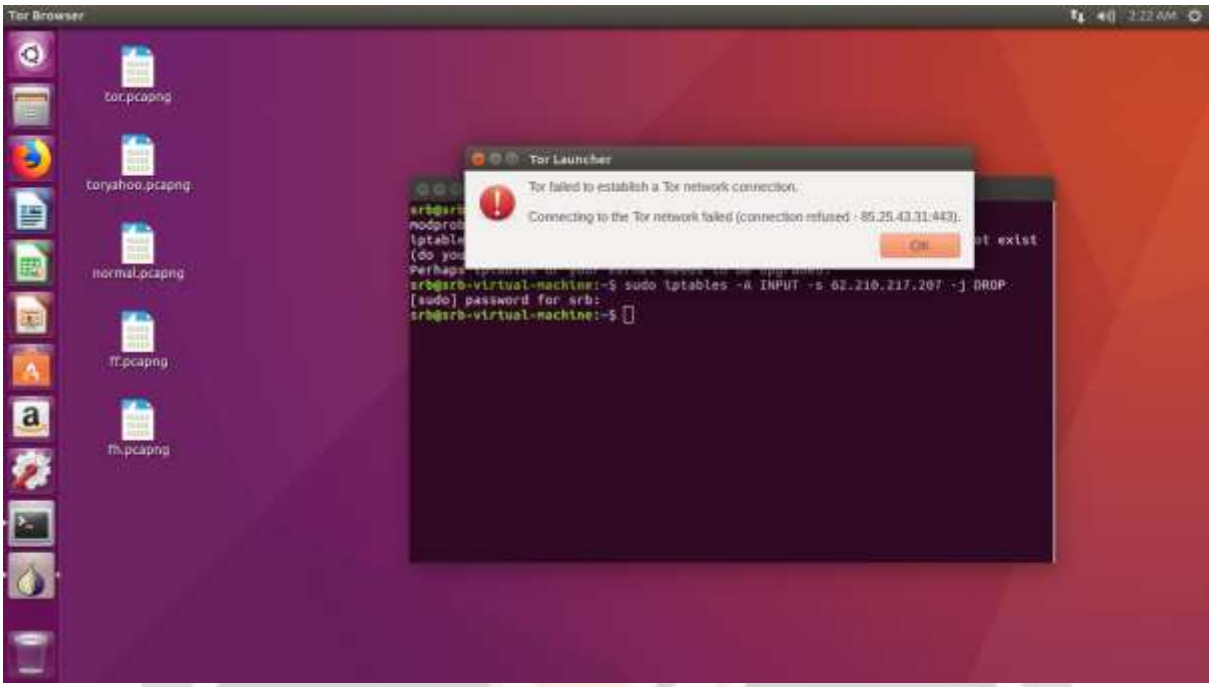

Fig -23: Connection to tor network is refused

5. PERFORMANCE ANALYSIS

Throughput: Network throughput is the rate of successful message delivery over a communication channel. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot.

Throughput = (RWIN/ RTT)

Where RWIN is the TCP Receive Window and RTT is the round-trip time for the path.

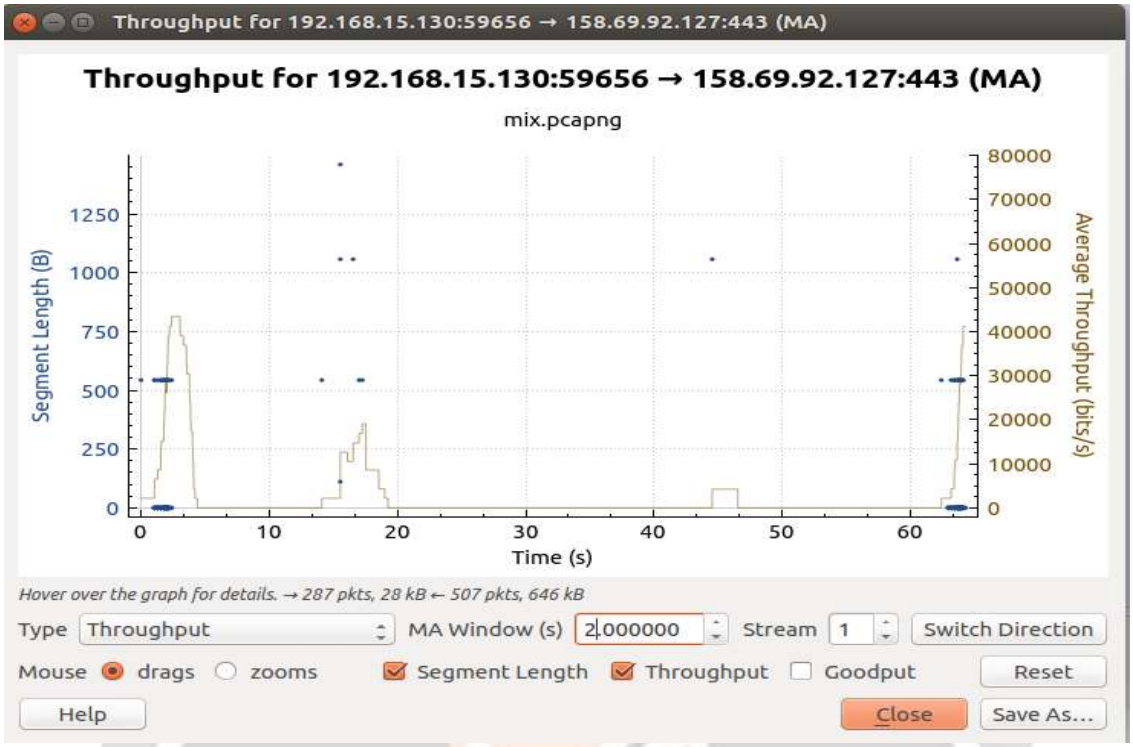

Fig -24: Throughput of implemented system

The above figure shows that the throughput of the network is less when there is presence of threats and anonymous TOR traffic in it. This can cause high bandwidth consumption and network congestion.

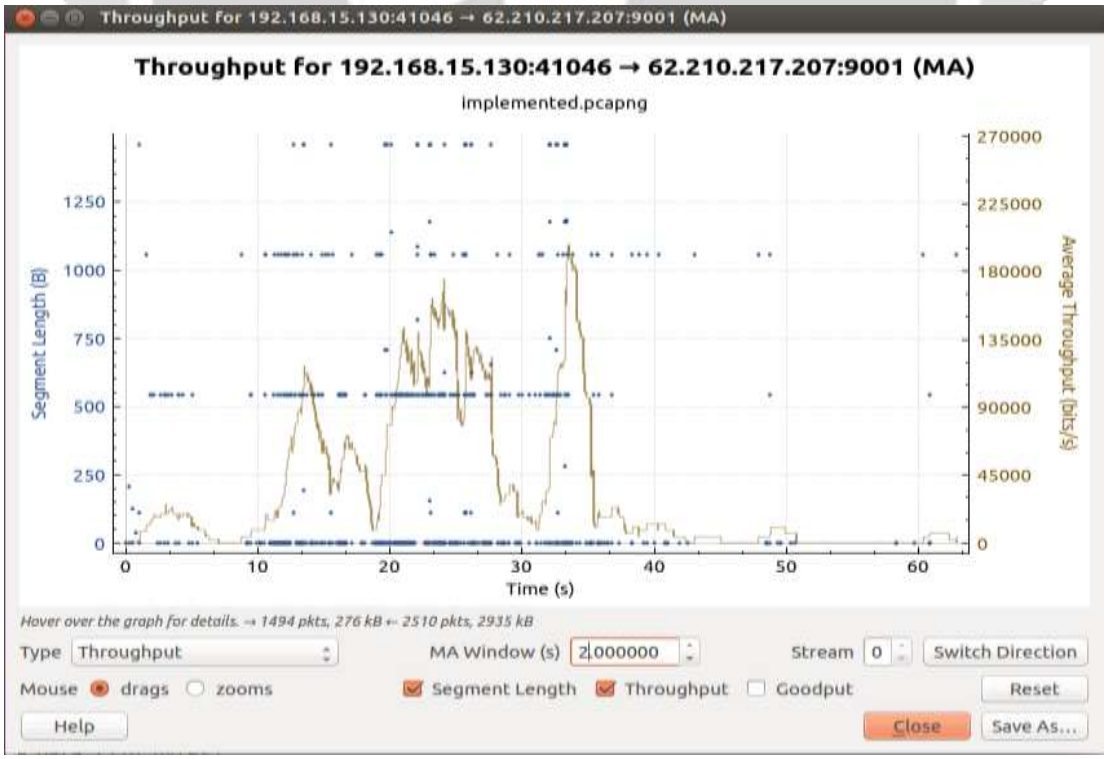

Fig -25: Throughput of implemented system

The above graph shows the improvement in the throughput of the existing system which is possible due to the implemented system as it blocks malicious traffic and TOR traffic. The implemented system enhances the throughput quite successfully.

6. CONCLUSIONS

The Suspicious activity in the network is a serious threat. The method which were used earlier, to identify the intrusion where not enough. The method which is proposed here, will first detect any suspicious threat or intrusions and then we add second-layer of security which is Deep Packet Inspection to make sure that the system will be free from any kind of threats. Hence the proposed system will improve the security and throughput of the network.

7. REFERENCES

[1] Basics of networking. Accessed by 10 January 2018 at <https://www.geeksforgeeks.org/basics-computer-networking/>

[2] Networking Equipment. Accessed by 12 January 2018 at <http://www.networking-basics.net/>

[3] Define Deep Packet Inspection. Accessed by 27 January 2017 at <https://en.wikipedia.org/wiki/Deep_packet_inspection>

[4] Deep Packet Inspection In brief. Accessed by 20 January 2017 at <http://computersecuritypgp.blogspot.in/2016/04/deep-packet-inspection.html>

[5] AbuHmed, T., Mohaisen, A. and Nyang, D., 2008. A survey on deep packet inspection for intrusion detection systems. *arXiv preprint arXiv:0803.0037*.

[6] Thant, M., Ye, K.Z., Thu, K.M. and Sin, S.T.T., 2016, April. Development of Firewall Optimization Model Using by Packet Filter. In *Computer Modelling and Simulation (UKSim), 2016 UKSim-AMSS 18th International Conference on* (pp. 273-278). IEEE.

[7] Deri, L., Martinelli, M., Bujlow, T. and Cardigliano, A., 2014, August. ndpi: Open-source high-speed deep packet inspection. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International* (pp. 617-622). IEEE.

[8] Mori, S., Sato, A. and Yoshida, K., 2016, January. Enhancingperformance of cardinality analysis by packet filtering. In *Information Networking (ICOIN), 2016 International Conference on* (pp. 23-28). IEEE.

[9] Parvat, T.J. and Chandra, P., 2014, December. Performance improvement of deep packet inspection for Intrusion Detection. In *Wireless Computing and Networking (GCWCN), 2014 IEEE Global Conference on* (pp. 224-228). IEEE.