Detecting and Blocking Encrypted Anonymous Traffic using Deep Packet Inspection

Parita Chandrakant Parekh¹, Prof. Jayshree Upadhyay²

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]

Deep Packet Inspection

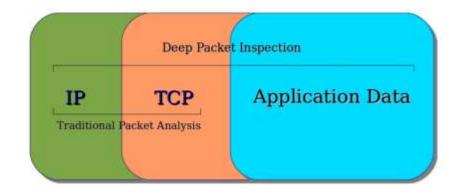


Fig -1: Deep Packet Inspection

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

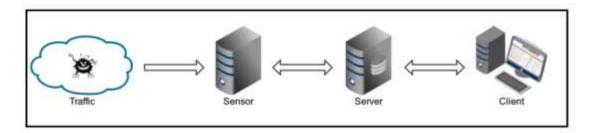


Fig -2: Architecture of MALTRAIL

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

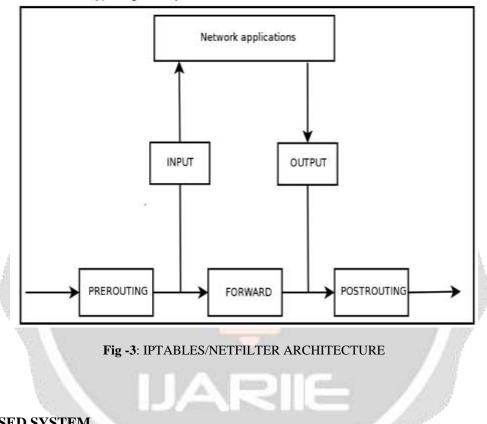
Deep packet inspection (DPI) is used to analyze the in-depth of the packets sent over the Internet.DPI bring he analysis of the content of the packet into the picture which used for the several purpose like Identifying the Malicious Packets, Intrusion, and many more for various types traffic management. 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.



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.

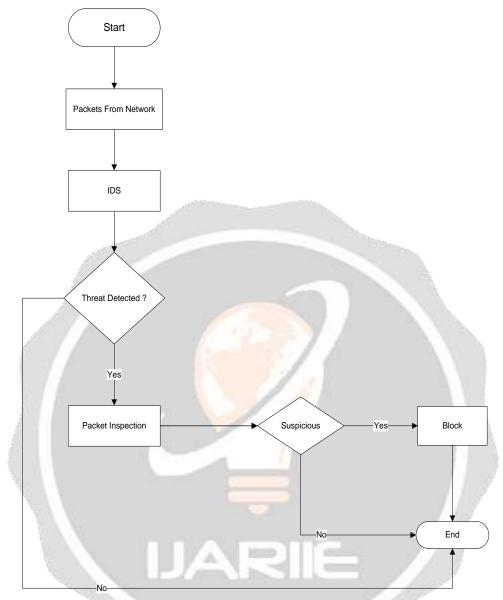


Fig -4: Flowchart of proposed system

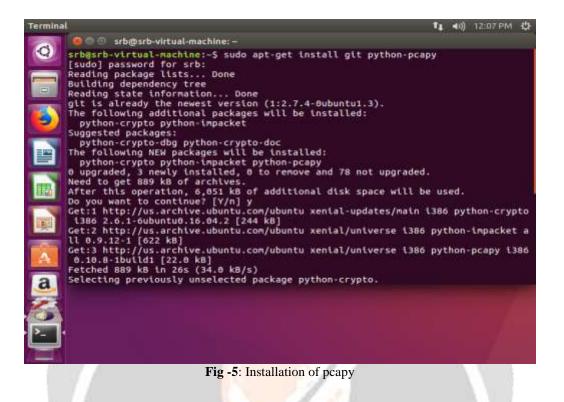
As mentioned, that system consist of two main parts: Detection Part and Inspection Part. In detection part, if the malicious packets are generated then detection system any suspicious activity is not detected, then it will drop the packet. If found some intrusion then further analyze, based on the packet 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



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



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

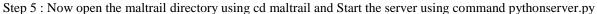


Sensor(s) is a standalone component running on the monitoring node (e.g. Linux platform connected passively to the SPAN/mirroring port or transparently inline on a Linux bridge) or at the standalone machine (e.g. Honeypot) where it "monitors" the passing Traffic for blacklisted items/trails (i.e. domain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



srbgisrb-virtual-machine: - /malitrali	11 40 1235PM Q
siberb-virtual-mechine:-f ad maltrall arberb-virtual-mechine:-/meltralis python server.py maltrall(server)#v0.10.316	
[1] using configuration file '/home/srb/maltrall/maltrall.conf' [1] starting HTTP server at 'http://0.0.0.0:8338/' [0] running [1]	
a	
🧭	
Fig -9: Start Maltrail server	

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

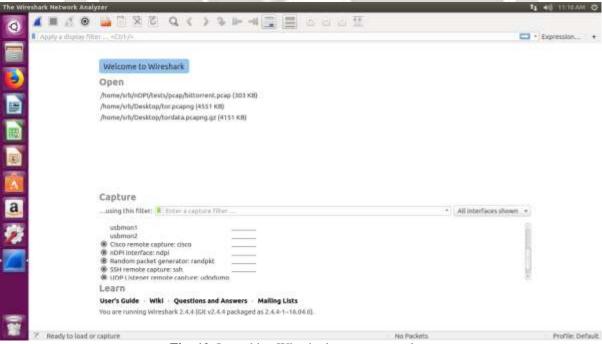


Fig -10: Launching Wireshark to capture packets

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



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

Maitrail (2018-03-22)	× +									
e + c @	() 127/0.0.1 (131)						🖾 🗘 🔍 740	rih	10. 0	0
- STatto				118-01-121	tatiwi 🔚			Concernant (THE SECOND	
	medium 		1 -#11							
2				Pilter		a	Class Print Touts			
- Brot seen dellant seenes		are joint i							reference 0	
1119 12 36 35 117 12 36 35 117 12 36 14 117 12 26 14	182.368,13.130.45	40590	83 210 217 507	BOUL	CMP TCP		62 210 217 207 million 207 154 206 118	tor and node inceptions	Alternapie de «11	H
111 12 23 47 111 12 29 57	192.168.11.197	400.94	198.181.101.58 882		EMP	ŏ	1.96.161.101.53	Making method insisares		h

Fig -12: Maltrail panel

th all sparses (b)

Source Destination Protocol Length Info	
	ication Data
	35538 [ACK] Seg=1 Ack=47 Win=64240 Len=8
	voted Alert
	- 35539 [ACK] Seg=1 Ack=78 Win=64240 Len=8
	- 443 [FIN, ACK] Seg-78 Ack=1 Win=65328 Lenge
184.27.191.236 192.168.15.139 TCP 68.443	
	- 35530 [FIN, FSH, ACK] Seg-1 Ack=79 Win=04238 Level
	- 443 [ACK] Seg=79 Ack=2 Win=65320 Len=8
	5 - 9001 [PSH, ACK] Seg=1 Ack=1 Win=65535 Len=543
	- 55576 [ACK] Seg=1 Ack=544 Min=64240 Len=0
A REAL PROPERTY AND A REAL	Source (Perc) and a Max-one approximate can-o
	0 - 443 [ACK] Seg=1 Ack=32 Min=39000 Len=0
	0 - 443 [FTW, ACK] Seg=1 Ack=32 Win=39680 Len=0
	- 50350 [ACK] Seg=32 Ack=2 Win=64239 Len=8
	- 55576 [PSH, ACK] Seg=1 Ack=544 Win=64248 Len=1428
	5 - 9001 [ACK] Seg=544 Ack=1421 Win=65535 Len=0
	- 55576 [PSR, ACK] Seg=1421 Ack=544 Win=64240 Len=14.
	0 - 9001 [ACK] Seg=544 Ack=2541 Min=65535 Len=0
	- 55576 [PSH, ACK] Seg=2841 Ack=544 Win=84240 Lem=787
	0 - 0001 [ACK] 10q=544 Ack=3628 WIN=66535 Len=0
	0 - 9001 [PSH, ACK] Seq=544 Ack=3828 Win=05535 Len=543
	- 55576 [ACK] Beg=3628 Ack=1087 Win=64248 Len=8
	- 55576 [PSH, ACK] 5eg=3628 Ack=1687 Win=64249 Len=1.
	- 55576 [PSH, ACK] Seg=5848 Ack=1087 Win=64249 Len=1.
	5 - 9001 [ACK] Seq=1007 Ack=6468 Win=65535 Len=0
a on wire (585 Gits), H5 Dytes captured (585 Gits) un interface 0 Veware Fc:1d:54 (68:65 Shiftidi5a), Dati Veware,cdiwDitb (00:0c Voriton 4, Src: 52:38:140 111, Dati 192.368:15:380 rol Protocol, frc Pert: 443, Dat Pert: 56388, Seq: 1, Ack: 1, Len yer Layer: Encrypted Alert	29:03:40:16}
s neither a field nor a protocol name.	ackets: 3705 - Displayed: 5705 (100.0%) - Load time: 0.4.531 Profile.

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

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

	5 🐵 📸 🖹 🕺 🗿 🔍 K 🗦 🦆 🛏 🗐 📰 🗇 🖂 🗃		= • Expression
	Welcome to Wireshark Open /home/srb/Desktop/boryahos.pcapig (3485.KB) /home/srb/Desktop/for.pcapig (4551.K0)		
	/home/sh/Oesktop/fli.pcapng (820 KB) /home/sh/Uesktop/ff.pcapng (1362 KB) /home/sh/Uesktop/nomal.pcapng (2405 KB)		
	/home/uh/hDPI/tests/pcap/toryahoo.pcapng (8174.68) /home/uh/hDPI/tests/pcap/tettorrent.pcap (363.68) /home/s/b/Desktop/tordata.pcapng.pz (not found)		
	Capture		
d		All interfaces shown	
	vsbmon2 Gisco remote cepture: disco ADPI interface: ndp1		Ĵ.
3	Extrap Invertise: Identification and pkt odpilleader wreisin working filter mate capture: odpidymp		
	odpineader		ų.

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

2 2	NO.	Time	Source	Destination		Langth info
3.0.251852 102.106.15.130 62.218.217.207 TCP 82.41848 - 9001 ACH Sep14 Ack+1 Min-92200 Lem-8 5.0.252863 62.219.217.207 102.106.15.138 Tor 83.9031 - 41046 FXR, MacK Sep14 Ack+205 Min-82200 Lem-8 6.0.252863 62.219.217.207 102.106.15.138 Tor 83.9031 - 41046 FXR, MacK Sep14 Ack+205 Min-82200 Lem-8 7.0.506285 132.106.15.138 62.219.217.207 TCP 82.41846 - 9001 FAR, MacK Sep120 Ack+205 Min-22900 Lem-8 10.509256 132.106.15.138 62.219.217.207 TCP 82.41846 - 9001 FAR, MacK Sep120 Ack+250 Min-22900 Lem-8 10.509256 122.106.15.138 62.219.217.207 TCP 82.41846 - 9001 FMR, MacK Sep170 Ack+234 Min-4248 Lem-8 10.6.763966 62.219.217.207 192.106.15.138 Tor 88.901 - 41046 FMR, AcK Sep170 Ack+234 Min-4248 Lem-8 110.6.763966 62.219.217.207 192.106.15.139 Tor 138.901 - 41046 FMR, AcK Sep170 Ack+237 Min-4248 Lem-8 120.762561 62.219.217.207 192.106.15.139 Tor 136.901 - 41046 FMR, AcK Sep190 Ack+237 Min-4248 Lem-8 13.014571 62.219.217.207	Para and	1 8.000000	192,308,35,138	82,218,217,297	TOP	182 41848 - 3081 [SYN] Hell-8 WIN-29100 Lee-8 MSS-1468 BACK P
A M 20/450 Disk 210 21/2 Disk 210/2 Disk 210/2 Disk 210/2 Disk 210/2						
b 0.252662 22.210.217.207 102.108.15.139 Ter 88.901410.46 Fex.8X Seq.1.46X-305	100	100 00 107 LT	110030510001015221000	CONTRACTOR DE LA CONTRACT		THE REPORT OF A DESCRIPTION OF A DESCRIP
6 9.300233 02.210.217.207 102.100.15.120 Tor 813.0001.41046 PSH, ACK Seq-1 Ack-200 Min-4248 Len 8 0.500336 102.106.15.139 02.210.217.207 TOR 813.001.41046 PSH, ACK Seq-1 Ack-200 Min-42960 Len 8 0.500375 132.106.15.139 02.210.217.207 TOR 206.41340 - 9001 PSH, ACK Seq-150 Min-42960 Len 10 0.703960 02.210.217.207 192.100.15.130 Tor 183.0001.41046 (PSH, ACK Seq-750 Ack-334 Min-40348 Len-8 10 0.703960 02.210.217.207 192.100.15.130 Tor 183.0001.41046 (PSH, ACK Seq-750 Ack-334 Min-40348 Len-8 11 0.763366 102.318.17.077 193.100.15.130 Tor 126.41046 - 9001 PSH, ACK Seq-750 Min-42348 Len-8 13 0.014571 62.210.217.207 193.100.15.130 Tor 1560.0011.44046 (PSH, ACK Seq-2217 Min-43248 Len-8 13 0.014571 62.210.217.207 193.100.15.130 Tor 1560.0011.44046 (PSH, ACK Seq-221 Ack-322 Min-43248 Len-9 13 1.014571 62.210.217.207 193.100.15.130 Tor 1562.00011.44046 (PSH, ACK Seq-227 Min-43248 Len-9 14 1.05099 62.316.217.207 192.100.15.130 Tor 1562.00011.44046 (PSH, ACK Seq-227 Min-43248 Len-9 15 1.01603 <td>1</td> <td>5 8.252662</td> <td>82.218.217.207</td> <td>192.168.15.130</td> <td></td> <td>88 9001 - 41046 [ACK] Seg=1 Ack=208 Win=64240 Len=8</td>	1	5 8.252662	82.218.217.207	192.168.15.130		88 9001 - 41046 [ACK] Seg=1 Ack=208 Win=64240 Len=8
7 9.504380 102.108.15.138 62.219.217.207 TCP 82.41540 9001 TCK1 5002380 Ack1 500380 Ack		6 0.505733		192.168.15.130	Tor	831 9801 - 41046 (PSH, ACK) Seg=1 Ack=208 Min=64248 Len=789
B 5000058 02.218.217.207 102.108.15.138 Ter 80.90005 00.01 Ack) Seq-334 Ack-334 Mine-61340 Lummed 10 0.750000 02.10.217.207 102.108.15.138 Tor 138.901 41046 [PSH, Ack] Seq-334 Ack_31001 Autmed240 Lummed240 11 0.752000 03.210.217.207 102.108.15.139 Tor 126.4046 PSH, Ack] Seq-334 Ack_372 Mine-6240 Lummed 13 1.04571 62.219.217.207 102.106.15.139 Tor 158.9001 -41046 [PSH, ACK] Seq-334 Ack=372 Mine-6240 Lummed 14 1.05590 62.219.217.207 102.106.15.139 Tor 158.9001 -41046 [PSH, ACK] Seq-324 Ack=372 Mine-6240 Lumed 151.018 Tor 158.9001 ACK] Seq-327 Mine-6240 Lumed 161.01806 Ack] Seq-327 Ack<2297		7 0.506280		62.218.217.287	TCP	82 41946 - 9001 [ACK] Seg=288 Ack=750 Win=29008 Len=8
10 0.753980 02.210.217.207 192.100.15.139 Tor 133.9001 -41040 Fesh, ACK Seq=750 AcK=334 Alimed248 L 11 0.753280 10.9.05.139 02.210.217.207 102.100.15.139 Tor 120.41046 ACK Seq=750 AcK Seq=750 AcK Seq=751 AcK Seq=752 AcK Seq=722 AcK AcK Seq=722 AcK Seq=722 AcK Seq=722		8 0.569375	192.168.15.130	62.210.217.207	for	208 41846 - 9001 [PSH, ACK] Seq=208 ACK=750 Win=29968 Len=12
110.765266 102.108.15.138 02.218.217.207 Ter 126.41646 - 5001 [Pier, ACK] Seq-334 Ack-851 Win-2096 L 130.752561 02.216.217.207 159.108.15.139 Ter 01001 - 41046 [ACK] Seq-3274 Ack-85124 Lensen 131.014571 02.216.217.207 159.108.15.139 Tor 1562.001 [ACK] Seq-2274 Ack-372 Win-64246 Lensen 151.015959 02.216.217.207 159.216.217.207 TCP 82.41046 - 5001 [ACK] Seq-372 Ack-3297 Win-64266 Lensen 151.015954 132.100.15.130 02.218.217.207 TCP 82.41046 - 5001 [ACK] Seq-372 Ack-3297 Win-64266 Lensen 161.016663 132.100.15.130 02.218.217.207 TCP 82.41046 - 5001 [ACK] Seq-372 Ack-3297 Win-82666 Lensen 161.016664 132.100.15.130 02.218.217.207 TCP 82.41046 - 5001 [ACK] Seq-372 Ack-3297 Win-82666 Lensen 161.016654 132.100.15.130 02.218.217.207 Ter 1554.41446 - 6001 [ACK] Seq-372 Ack-3297 Win-82666 Lensen 161.017021 02.218.217.207 152.108.15.130 Ter 86.9001 - 41046 [ACK] Seq-3297 Ack-3832 Win-84266 Lensen 161.017026 02.218.217.207 152.108.15.130 Ter 86.9001 - 41046 [ACK] Seq-3297 Ack-3433 Win-84266 Lensen 201.551564 02.218.217.207 152.108.15.130 Ter 86.9001 - 41046 [ACK] Seq-3297 Ack-3433 Win-84268 Lensen 221.550531 132.106.15.130 02.218.217.207 Ter 1323 9410 - 41046 [ACK] Seq-3297 Ack-3433 Win-84268 Lensen 221.550531 132.106.15.130 Ter 80.9001 - 41046 [ACK] Seq-3297 Ack-3434 Win-84248 Lensen 221.550531 132.106.15.130 Ter 1339 100.15.130 Ter 80.9001 - 41046 [ACK] Seq-3297 Ack-3433 Win-84248 Lensen 221.550531 132.106.15.130 03.218.217.207 Ter 1323 941468 - 5001 [Pier, ACK] Seq-3297 Ack-3434 Win-35948 221.550423 02.218.217.207 192.108.15.130 Ter 80.9001 - 41046 [ACK] Seq-3297 Ack-3434 Win-84248 Lensen 231.851498 02.218.217.207 192.108.15.130 Ter 80.9001 [Hier, ACK] Seq-3354 Ack-3500 Win-64248 Lensen 231.854930 132.106.15.138 03.218.217.207 Tor 625 41046 - 5001 [Pier, ACK] Seq-3354 Ack-3509 Win-64248 Lensen 231.85493 132.106.15.139 03.218.217.207 Tor 625 41046 - 5001 [Pier, ACK] Seq-3354 Ack-3509 Win-64248 Lensen 251.85493 132.106.15.139 03.218.217.207 Tor 625 41046 (ACK] Seq-3354 Ack-3500 Win-64248 Lensen 251.85493		9.0.509856	62.218.217.207	192.168.15.139	Tor	88 0001 - 41045 [ACK] 5eq=750 Ack=334 Win=64240 Len=8
10 0.752360 02.218.217.207 192.108.15.139 Ter 08 1001 - 41046 CACK) Seq-801 Ack-372 Mim-62240 Lum-8 13 1.014571 62.259.217.207 192.108.15.139 Tor 1562 0801 - 41046 FRM, ACK) Seq-801 Ack-372 Mim-62240 Lum-8 14 1.615939 62.218.217.207 192.108.15.139 Tor 1582 0801 - 41346 FRM, ACK) Seq-8172 Ack-272 Mim-62240 Lum-8 15 1.615954 192.108.15.130 62.218.217.207 TCF 82 41468 - 9001 ACK) Seq-372 Ack-2297 Mim-32000 Lem-9 16 1.015083 192.108.15.130 62.218.217.207 Tor 154.41846 - 9001 ACK) Seq-372 Ack-2297 Mim-32000 Lem-9 17 1.016954 192.108.15.130 62.218.217.207 Tor 154.41846 - 9001 ACK) Seq-3297 Ack-132 Mim-64248 Lum-9 18 1.017021 62.216.217.207 192.108.15.138 Tor 88 9011 - 41046 ACK) Seq-2297 Ack-132 Mim-64248 Lum-9 20 1.555164 02.218.217.207 192.108.15.138 Tor 1129 41046 - 9001 FPM, ACK Seq-2297 Ack-132 Mim-64248 Lum-9 21 1.550801 112.108.15.138 Dor 1129 41046 - 9001 FPM, ACK Seq-2297 Ack-1344 Mim-64248 Lum-9 2		18 0.763060	62.210.217.207	192.100.15.130	TOF	133 9001 - 41046 [PSH, ACK] Seq=750 Ack=334 Win=64240 Len=51
131.014571 62.210.217.207 192.108.15.130 Tor 1562.001 464.5099 62.216.217.207 192.108.15.130 Tor 1568.001 41.046 [FSH, ACK] Seq=201 Act=372 Win=60248 L 151.013094 132.108.15.130 02.218.217.207 TCF 82.41048 5001 ACK] Seq=2127 Act=322 Win=60248 L 151.013094 132.108.15.130 02.218.217.207 TCF 82.41048 5001 ACK] Seq=3227 Act=3227 Win=32060 Lenee 10.010654 192.108.15.130 02.218.217.207 Tor 1542.41046 5001 ACK] Seq=3297 Act=3237 Win=32660 Lenee 11.010654 192.108.15.130 02.218.217.207 Tor 1542.41046 5001 ACK] Seq=2297 Act=3232 Win=64248 Lenee 121.010702 62.218.217.207 192.108.15.130 Tor 80901 41046 ACK] Seq=2297 Act=332 Win=64248 Lene 21.551544 02.218.217.207 192.108.15.130 Tor 1339.9901 41046 ACK] Seq=2297 Act=343 Win=64248 Lene 21.550551 12.208.15.130 Tor 1339.9901 41046 ACK] Seq=2297 Act=343 Win=64248 Lene 22.1550551 12.00.15.130 Tor 1339.9901 41046 ACK] Seq=3207 Act=343 Win=64248		11.0.763266	192.168.15.138	62.218.217.207	Tor	
14.815939 62.218.117.207 102.108.15.130 Tor 158.901 -41046 [PeH, ACK] Seq=2211 Ack=172 Win=04246 15.1.013084 192.108.15.130 02.218.217.207 TCF 82.41048 -9001 [ACK] Seq=722 Ack=2297 Min=12068 Len 16.1.0140843 192.108.15.130 02.218.217.207 Tor 1542.41846 -9001 [ACK] Seq=722 Ack=2297 Min=12068 Len 17.1.014054 192.108.15.130 02.218.217.207 Tor 1542.41846 -9001 [ACK] Seq=7227 Ack=2297 Min=12068 Len 18.1.017026 62.218.217.207 192.108.15.138 Tor 08.9001 -41046 [ACK] Seq=7227 Ack=1332 Min=04248 Len 29.1.551544 02.218.217.207 192.108.15.138 Tor 08.9001 -41046 [ACK] Seq=7297 Ack=1333 Min=04248 Len 21.1.550544 02.218.217.207 192.108.15.138 Tor 08.9001 -41046 [ACK] Seq=7297 Ack=1333 Min=04248 Len 22.1.9207 2.218.217.207 192.108.15.138 Tor 08.901 -41046 [ACK] Seq=7304 Ack=3354 Win=3548 Min=04248 Len 23.1.820438 62.218.217.207 192.108.15.138 Tor <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td></td<>						
15.1.013054 112.100.15.130 02.210.217.207 TCF 82.41040 - 9001 ACK) Seq-2297 Ack-1200 Mini-12000 Lenne 16.1.0130643 192.100.15.130 00.210.217.207 Tor 152.41040 - 9001 ACK) Seq-2297 Ack-1200 Mini-12000 Lenne 17.1.010054 192.100.15.130 05.210.217.207 Tor 152.41040 - 9001 PSH, ACK) Seq-2297 Ack-1202 Mini-12000 Lenne 18.1.017026 02.210.217.207 192.100.15.130 Tor 80.9001 - 41046 ACK) Seq-2297 Ack-1202 Mini-4200 Lenne 20.1.551564 02.210.217.207 192.100.15.130 Tor 80.9001 - 41046 ACK) Seq-2297 Ack-1203 Mini-62240 Lenne 20.1.551564 02.210.217.207 192.100.15.130 Tor 130.9001 - 41046 ACK) Seq-2297 Ack-1943 Mini-64240 Lenne 21.550501 112.00.15.130 Tor 1139.9001 - 41046 ACK) Seq-2297 Ack-1943 Mini-64240 Lenne 22.1.560423 02.210.217.207 192.100.15.130 Tor 1139.9001 - 41046 ACK) Seq-2207 Ack-1943 Mini-64240 Lenne 23.1.560430 192.100.15.130 Tor 130.9001 - 41046 FSH, ACK) Seq-2354 Ack-19060 Mini-64240 Lenne						
16 1.050063 192.100.15.130 02.210.217.207 Tor 1542.41846 - 9001 [Ack] Seq-372 Ack-2207 Min-32000 17 1.010954 192.100.15.130 02.210.217.207 Tor 1543.41866 - 9001 [Ack] Seq-3272 Ack-2207 Min-32000 18 1.017026 02.210.217.207 192.100.15.138 Tor 88.9011 - 41046 [Ack] Seq-3297 Ack-1303 Min-32000 19 1.017026 02.210.217.207 192.100.15.138 Tor 88.9011 - 41046 [Ack] Seq-3297 Ack-1303 Min-64248 20 1.551564 02.210.217.207 192.100.15.130 Tor 1339.9001 - 41046 [Ack] Seq-2297 Ack-1303 Min-64248 21 1.555051 192.100.15.139 62.218.217.207 Ter 1339.9104 - 40046 [Ack] Seq-2297 Ack-1354 Min-64248 21 1.555051 192.100.15.139 62.218.217.207 Ter 1339.9104 - 40046 [Ack] Seq-3000 Min-64248 Min-64248 21 1.555051 192.100.15.130 Tor 62.9001 - 41046 [Ack] Seq-3000 Min-64248 Min-64248 21 1.555054 62.219.217.207 192.100.15.130 Tor 62.9001 - 41046 [Ack] Seq-3000 Min-64248 Min-64248 21 1.555054 62.219.217.207 192.100.15.130 Tor 62.9001 - 41046 [Ack]						
17 1.010954 192.108.15.138 02.218.217.207 Tor 192.41840 - 9001 [PSP, ACK] Seq=2327 Ack=1297 Min=32008 18 1.017021 02.210.217.207 192.108.15.138 Tor 80.9011 - 41046 [ACK] Seq=2207 Ack=1343 Min=64248 Lem-20 1.551544 19 1.017026 02.219.217.207 192.108.15.138 Tor 80.9011 - 41046 [ACK] Seq=2207 Ack=1343 Min=64248 Lem-20 1.551564 20 1.551564 02.219.217.207 192.108.15.130 Tor 103.9001 - 41046 [ACK] Seq=2207 Ack=1343 Min=64248 Lem-20 1.551564 21 1.553651 102.108.15.130 Tor 113.99011 - 41046 [ACK] Seq=2207 Ack=1343 Min=64248 Lem-20 1.55154 22 1.55051 102.108.15.130 Tor 113.99011 - 41046 [ACK] Seq=2354 Ack=3000 Min=64248 Lem-20 1.55154 23 1.550452 02.219.217.207 192.108.15.130 Tor 08.0001 - 41046 [PSH, ACK] Seq=2354 Ack=3000 Min=64248 Lem-20 1.55154 23 1.550459 02.219.217.207 192.108.15.130 Tor 02.541264 - 3001 [PSH, ACK] Seq=3354 Ack=3000 Min=64240 Lem-20 1.55154 24 1.8535051 192.2168.15.138 03.218.217.207 Tor 02.541264 - 3001 [PSH, ACK] Seq=3354 Ack=3300 Min=64240 Lem-20 1.55154 25 1.354128 05.218.217.207 192.108.15.138 Tor 02.541264 - 3001 [PSH, ACK] Seq=3354 Ack=3300 Min=64240 Lem-20 1.55168 21						
18 1.017021 02.210.217.207 102.108.15.130 Ter 08.0001 +41046 [ACK] 5eq=2297 Ack=1332 Min=64248 Lem- 20 19 1.017026 62.216.217.207 102.108.15.130 Ter 08.0001 +41046 [ACK] 5eq=2297 Ack=1332 Min=64248 Lem- 20 20 1.551544 62.216.217.207 109.108.15.130 Ter 1135 9001 +41046 [PSH, ACK] 5eq=2297 Ack=1343 Min=64248 Lem- 20 1.551544 62.216.217.207 109.2108.15.130 Ter 1139 9001 +41046 [ACK] Seq=2297 Ack=1343 Min=64248 Lem- 20 1.551544 62.218.217.207 Ter 1139 9101 +41046 [ACK] Seq=2297 Ack=1364 Min=64248 Lem- 20 Ack Seq=2297 Ack=1364 Min=64248 Lem- 21 Ack Seq=2297 Ack Seq=2297 Ack Seq=2297 Ack Min=64248 Lem- 21 Ack Seq=2697 Ack Seq=2697 Ack Min=64248 Lem- 21 Ack Seq=2697 Ack Min=64248 Lem- 21 Ack Seq1448						
19 1.017026 62,218.217.207 192,108.15.138 Ter 08 0001 41046 [CK] Seq-3207 Ack+1043 Minne6424H Lem- 201,550544 201,550544 00,218.217.207 192,108.15.138 Tor 1139 40046 [PSH, ACK] Seq-2197 Ack+1043 Minne6424H Lem- 211,5508031 211,5508031 192,108.15.138 02,218,217.207 Ter 1139 41046 -0001 [PSH, ACK] Seq-2194 Ack+3354 Minne3428H Lem- 3508 221,550423 02,218,217.207 192,108.15.138 Ter 08 1001 -41046 [PSH, ACK] Seq-2194 Ack+3354 Minne3428H Lem- 3518 231,550423 02,218,217.207 192,108.15.138 Tor 08 1001 -41046 [PSH, ACK] Seq-3154 Ack-3060 Minne6428 Lem- 361.35380 241,853803 192,148.15.138 03,218,217,207 Tor 625 41248 - 5001 [PSH, ACK] Seq-3287 Ack-3349 Min-335848 251,354128 62,310,217,207 192,108.15.138 Ter 08 1001 41046 [ACK] Seq-3287 Min-33648 261,3542128 62,310,217,207 192,108.15.138 Tor 80 991 43046 [ACK] Seq-3897 Min-38348 271,9991226 62,310,217,207 192,108.15.138 T						
201.551544 02.13.8.217.007 102.108.15.130 Tor 1135.9001 +104.6 [FSH, ACK] Seq=2207 Ack=1343 Minmed240 211.555054 102.108.15.130 02.218.217.207 102.108.15.130 Tor 1135.9001 +104.6 [FSH, ACK] Seq=2207 Ack=1343 Minmed240 221.550053 02.218.217.207 102.108.15.130 Tor 01.001 +41.04.6 [FSH, ACK] Seq=23054 Ack=3060 Minmed240 Lum 221.550052 02.218.217.207 102.108.15.130 Tor 625.401.44.6 FSH, ACK] Seq=33054 Ack=3060 Minmed240 Lum 241.855801 152.168.15.130 02.218.217.207 Tor 625.41046 -9001 [FSH, ACK] Seq=3807 Ack=3064 Lum 251.854118 67.218.217.207 192.108.15.130 Tor 625.41046 -9001 [FSH, ACK] Seq=3807 Ack=3064 Lum 251.8544118 67.218.217.207 192.108.15.130 Tor 625.41046 -9001 [FSH, ACK] Seq=3807 Ack=3369 <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td></td<>						
211.5558831 1102.108.15.138 62.218.217.207 Ter 1139.41448 - 9001 [F94, ACK] Seq:1343 Ack:3354 Min-33588 221.5568032 02.219.217.207 150.108.15.138 Ter 01001 - 41046 [ACK] Seq:13154 Ack:3306 Min-64248 231.856498 62.219.217.207 192.108.15.138 Ter 01001 - 41046 [ACK] Seq:13354 Ack:3306 Min-64248 241.853801 132.108.15.138 02.218.217.207 192.108.15.138 Ter 0010 [F94, ACK] Seq:3354 Ack:3306 Min-64248 251.854438 62.210.217.207 192.108.15.138 02.218.217.207 Ter 01001 - 41046 [ACK] Seq:3304 Ack:3304 Min-53348 251.854438 62.210.217.207 192.108.15.138 Ter 01001 - 41046 [ACK] Seq:3304 Ack:3304 Min-53348 251.850408 192.108.15.138 Ter 01001 - 41046 [ACK] Seq:3314 Ack:3304 Min-53348 261.830408 192.108.15.138 Ter 025.41846 - 9001 [F84, ACK] Seq:3314 Ack:3304 Min-54248 271.9971226 02.218.217.207 192.108.15.138 Ter 825.0001 - 41046 [ACK] Seq:3207 Ack:4008 Min-64248 28.2.111878 02.218.217.207 192.108.15.138 Ter 825.0001 - 41046 [ACK] Seq:3207 Ack:4008 Min-64248 29.1.11878 02.218.217.207 192.108.15.138 Ter 825.0001 - 410						
22 1.560423 02.210.217.207 102.100.15.130 Tor 00.100.16.140.0CK) Sept3354 Ack-3000 Win-64240 Lum- 23 1.550430 02.210.217.207 102.100.15.130 Tor 025.6001 - 41046 [FSH, ACK] Sept3354 Ack-3000 Win-64240 Lum- 24 1.553801 152.160.15.130 02.210.217.207 Tor 025.41846 - 3001 [FSK, ACK] Sept3354 Ack-3000 Win-64240 Lum- 25 1.364138 03.210.217.207 159.100.15.130 Tor 00.0001 - 41046 [ACK] Sept-3007 Ack-3059 Win-63240 27 1.951226 02.210.217.207 159.100.15.130 Tor 025.41846 - 3001 [FSK, ACK] Sept-3007 Ack-3059 Win-64240 Lum- 20 1.360080 109.160.15.130 02.210.217.207 Tor 025.41846 - 3001 [FSK, ACK] Sept-3007 Ack-3058 Win-64240 Lum- 20 1.360080 109.160.15.130 109.210.217.207 Tor 025.41846 - 3001 [FSK, ACK] Sept-3007 Ack-4068 Win-64240 Lum- 20 1.360080 109.160.15.130 109.210.217.207 Tor 025.41846 (ACK] Sept-3007 Ack-4068 Win-64240 Lum- 20 1.360080 109.160.15.130 109.210.217.207 Tor 025.41846 (ACK] Sept-3007 Ack-4068 Win-64240 Lum- 20 1.360080 109.160.15.130 109.100.15.130 Tor 025.41846 (ACK] Sept-3007 Ack-4068 Win-64240 Lum- 20 1.360080 109.210.217.207 109.100.15.130 Tor 025.41846 (ACK] Sept-3007 Ack-4068 Win-64240 Lum- 20 1.360080 109.210.217.207 109.100.15.130 Tor 025.41846 [FSK, ACK] Sept-3007 Ack-4068 Win-64240 Lum- 20 1.1877 Ack-4058 Win-64240 Lum- 20 1.1877 Ack-4058 Win-64240 Lum- 20 1.1877 Ack-4058 Win-64240 Lum- 20 1.1878 Ack - 3600.10.100.00.100.100.00.100.100 [FSL 400.200 [FSL 400						
23 1.854498 62.210.217.207 192.108.15.138 Tor 625.001 - 41046 [FSA, ACK] Seq=3854 Ack-3000 Win-66428 24 1.853801 192.108.15.138 02.218.217.207 Tor 625.41046 - 9001 [FSA, ACK] Seq=3805 Ack-3809 Win-56428 25 1.854138 62.210.217.207 192.108.15.138 Ter 68.0001 - 41046 [ACK] Seq=3007 Ack-3243 Win-564240 26 1.950080 192.108.15.138 02.218.217.207 Tor 625.41846 - 9001 [FSA, ACK] Seq=3807 Ack-3243 Win-564240 27 1.990226 62.210.217.207 192.108.15.138 Tor 82.9901 - 41046 [ACK] Seq=3807 Ack-4008 Win-664240 28 2.113878 62.210.217.207 192.108.15.138 Tor 82.9901 - 41046 [ACK] Seq=3807 Ack-4008 Win-664240 28 2.113878 62.210.217.207 192.108.15.138 Tor 82.9901 - 41046 [ACK] Seq=3807 Ack-4008 Win-664240 Frame 4: 289 bytes on wire (2312 hits), 289 bytes captured (2312 hits) on interface 8 Ethermet 17, Sec: Weare, c3.49:10 (00:00:22.02.43.010, b). Dit Wmare, fr.104/54 (00:50:56.16.10.158) Ditermet Fraucol Version 4, Sec: 192.108.15.13.03						
241.853800 192.168.15.138 02.218.217.207 Tor 625.41248 - 9001 [Psr, ACK] Seq-3800 ACK-3897 Min-38348 251.85418 07.210.217.207 193.100.15.138 Tor 00.0001 - 41046 [ACK] Seq-3807 ACK-3858 Min-64240 Len-261.990226 02.210.217.207 192.100.15.138 Tor 025.41846 - 9001 [PsH, ACK] Seq-3807 ACK-3858 Min-64240 Len-287.1391226 02.210.217.207 192.100.15.138 Tor 025.41846 - 9001 [PSH, ACK] Seq-3807 ACK-4086 Min-64240 Len-287.13978 02.210.217.207 192.100.15.138 Tor 025.41846 - 9001 [PSH, ACK] Seq-3807 ACK-4086 Min-64240 Len-287.13978 02.210.217.207 192.101.5.138 Tor 025.001 - 41046 [PSH, ACK] Seq-3807 ACK-4086 Min-64240 Len-287.001 - 41045 [PSH, ACK] Seq-3807 ACK-4086 Min-64240 - 41046 [PSH, ACK] Seq-3807 ACK-4086 Min-64240 - 4104 - 41046 [PSH, ACK] Seq-3807 ACK-4086 Min-64240 - 4104 - 41046 [PSH, ACK] Seq-3807 ACK-4086 Min-64240 - 4104 - 41046 [PSH, ACK] Seq-3807 ACK-4086 Min-64240 - 4104 - 4						
251.854118 62.210.217.307 189.100.15.138 Ter 00.0000-41046 ACKI Seq-3007 Ack+3545 Win-04240 Len-20 1.900400 201.950080 192.100.15.130 02.210.217.207 Tor 02.61946 - 9001 JPSH, ACKI Seq-3007 Ack+3554 Ack=3837 Win=38348 271.951226 62.210.217.207 199.100.15.138 Tor 88.9901 - 41046 JACKI Seq=3007 Ack+4058 Win=64240 Len-20.21.317.207 28.113578 02.210.217.207 199.100.15.138 Tor 88.9901 - 41046 JACKI Seq=3007 Ack+4058 Win=64240 Len-20.21.315.78 28.2.113578 02.210.217.207 199.100.15.138 Tor 82.9901 - 41046 JACKI Seq=3007 Ack+4058 Win=64240 Len-20.21.315.78 7Frame 41.2045 JPSH, ACKI Seq=3007 Ack+4058 Win=64240 Len-30.42.100.11.30 Tor 82.9901 - 41046 JACKI Seq=3007 Ack+4058 Win=64240 Frame 41.209 bytes on wire (2312 hits), 289 bytes captured (2112 hits) on interface 8 Ethermet 11, Sec Venuere (23.42.10 (0.00.20.23.43.10), bit Venuere (71.104.54 (00.56.56.56.56.56.56.56.56.56.56.56.56.56.						
201.999080 192.160.15.138 02.218.217.207 Tor 625.41846 -9001 [FSH_ACK] ACK] Sequ-3543 Ack=3897 Min=38348 271.990206 02.210.217.207 192.100.15.198 Tor 88.9001 41.0046 JACK] Sequ-3503 F Min=38348 28.2.111878 02.210.217.207 192.100.15.138 Tor 88.9001 41.0046 JACK] Sequ-3503 F Ack=4006 Min=64240 28.2.111878 02.210.217.207 192.100.15.138 Tar 87.9001 41.046 JACK] Sequ-3503 F Ack=4006 Min=64240 Frame 4: 269 bytes on wire (2312 hits), 289 bytes captured (2312 hits) on interface 8 Ethermet T1, Sec: Venuere (-3.40-16 (10.10.30) Det (-5.21.01.51.01.51) Different T1, Sec: Venuere (-5.40-16 (10.10.130) Det (-5.21.27.207 21.01.51.30) Det (-5.21.56) fc.1d.5a) Different T2, Sec: Venuere (-5.40-16 (10.10.130) Det (-5.21.27.207 21.01.51.30) Det (-5.21.56) fc.1d.5a)						
27 1.901226 62.210.217.207 102.108.15.138 Tor 88.901. +1046 [ACK] 9012807 Ack=4006 Min=64246 Lent 28 2.113878 02.210.217.207 192.108.15.138 Tar 82.901. +1046 [PSH, ACK] Seq=3807 Ack=4006 Win=64246 Lent 77 as 02.210.217.207 192.108.15.138 Tar n21.001.1 41046 [PSH, ACK] Seq=3807 Ack=4006 Win=64248 Frame 4.369 Uptes on wire (2312.015.) 289.011.15.138 on interface # Ethernet II. Src: Venure_01.6(00.00.291c3.4816.) Delt Venure_1c1.14(56.00.500.56.16.104.) Delt Venure_1c1.14(56.00.56.16.104.) Delt Venur						
28 2.111878 02.210.217.287 192.188.15.138 Ter 825.0001 - 41045 [PSH, ACK] Seq-3007 Ack-4008 Win=64268 Frame 4: 289 bytes on wire (2812 hits), 289 bytes captured (2312 hits) on interface 8 Ethermet Tr, Sec: Venuere c5.49-16 (00:00:29:03.400.16), Doi: Venuere fr.14(56 (00:56:56:fc:14:56)) Determet Protocol Version 4, Sec: 182.100.15.130, Doi: 05.237.207						
Frame 4: 200 bytes on wire (2312 bits), 200 bytes captured (2312 bits) on interface 0 Ethermet II, Src: Vmwure_c3:a9:10 (00:00:29(c3:a9:10), Dat: Vmwure_fc:1d:5a (00:50:56:fc:1d:5a) Ditermet Protocol Version 4, Src: 192.(00:15:130, Dat: 62.230-237.207						
Elhernet II, Src: Vmwure_c3:a9:16 (00:00:29:c3:x0:16), Det: Vmwure_fc:1d:5a (00:50:56:fc:1d:5a) Internet Protucol Version 4, Src: 192.100.15.130, Det: 62.210.217.207	1 prime	20 2.1115/8	02.210.217.207	193.100.15.100	1007	HIZ DORT - ETONO [PSH, HUN] SEG-SON/ ACK-BOOK WIN-BOARN LUD-
Data (207 bytes)	▶ 武 ▶ 30	20 2.111878 ame 4: 289 byte hernet II, Src; ternet Protucol ansmission Cont	62.218.217.207 s on wire (2312 hits) Vmwure_c3:a9:16 (00: Version 4, Src: 192	192.108.15.130 . 289 bytes captored 0c.29(c3:x8:16), Dati 160.15.130, Dati 62.2	Tor (2312 bits Vesars_fc 10.217.207	825 8881 - 43045 [PSH, ACK] Seg-3897 Ack-4008 Min=64248 Lan- on interface 8 Id.5a (00:50:56;fc:Id.5w)
and Respect		nt. newseal				
Fig -15: Deep Packet Inspection showing TOR IP's	0.7	wirsshark wirsto				

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

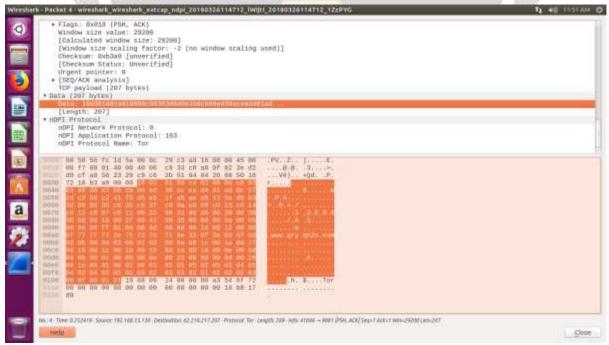


Fig -16: Breakdown of TCP [Protocols in frame: eth:ethertype:ip:tcp:data]

a tuble h a dol	Shinds And Kill. 1	. «Drivle					Expression.
Time		Source	Destination	+ Protocol	Length info		
3797 33.3	393394	102.168.15.130	62.210.217.207	100	82 41040 - 0001	[ADK]	Seq=356140 Ack=2816271 Min=65535 Len=0
3800 31,3	397917	192.168.15.139	62.210.217.207	TOP	82 41040 - 9001	[ACK]	Seg=256140 Ack=2821111 Min=05535 Len=0
3803 33.4	491268	192.168.15.130	62,210,217,297	TOP			Seq=256140 Ack>2823951 Win=65535 Len=0
3864 33.4	481593	102.168.15.138	62.210.217,207	Tor		[PSH,	ACK] 5eq=250148 Ack=2823951 Min=05535 Len=
3810 33.4	487872	107, 168, 15, 130	62.210.217.207	TEP	82 45646 - 9991	(ACK)	Seg-757748 Ack+2826831 Min+65535 Len+8
3813 33.4	411948	152.168.15.138	62.210.217.207	TOP			5eg=257748 Ack=2828612 M1#=85535 LeH=8
3815 33,4	427725	192.168.15.139	62.219.217.207	Tor	625 41946 - 9891	EPSH,	ACM] Seg=257740 Ack=2830032 Win=65535 Len=
3819 33.4	438777	192.168.15.139	63,230,237,207	TOP	82 41046 - 0001	CAPT'T.	the contraction of the boundary of the second second
3822 33.4	are parallely	192.168.15.138	with march interfer march			<pre>()</pre>	Seq=258383 Ack+2832872 Min=65535 Len=0
	450990	100.100.10.100	62.210.217.287	TOP	82 41646 - 9881		Seq=258283 Ack=2835712 Min=65535 Len=6
3824 33.4		192.100.15.130	62.210.217.207	TOP		[ACK]	
3824 33.4 3828 33.4 Encape Arriva (Time (Time (Time	aB7484 ab1379 al Time: 4 shift for Time: 15: delta fro delta fro	192.300.15.130 192.308.15.130 type: Ethernet (1) 4or 26, 2018 11.45.1 this packet: 0.000 22009912.277957000 s mp previous captured mp previous captured	62,210,217,207 62,210,217,207 62,210,217,207 600000 seconds] econds frame: 0.000725000 d frame: 0.000725000	Tor TCP seconds]	625 41646 - 9981	[ACK] [PSH,	Seq=258283 Ark=2835712 Win=65535 Len=8
BE24 33 - 4 BE26 33 - 4 Encapos Arrigos (Time Encapos (Time Encapos (Time Frame Frame Frame (Frame (Frame (Frame (Frame (Frame (Color) (Color) Ethermet Statarov (Color) (abraba ability whist for the is delta fro delta fro delt	192.300.15.139 192.308.15.139 type:Ethernet(1) for 26, 2018 11.45:1 this packet:0.000 22089952.277957000 0 mp previous captured mp previous capture	02.210.217.207 62.210.217.207 62.217.057966 P07 600000 seconds] cconds frame: 0.000725000 d frame: 0.000725000 me: 33.482454090 sec \$) its}	Tor ICP seconds] + seconds] and\$]	025 11846 - 9001 82 41048 - 9001	(ACK) (PSH, (ACK)	Seq=256283 Ark=2835711 Min=65535 Len=8 ACA] Seq=298283 Ark=283732 Min=65535 Len=8 Seq=256826 Ark=2830072 Min=65535 Len=8

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

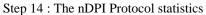
As shown in figure the format for Tor frame is [Protocols in frame: eth:ethertype:ip:tcp:data] where data is suspiciously attached as the frame in normal packet shows itself as TCP but in Deep Packet Inspection we find that it is not TCP and originally it is TOR

Q 🐔 🗏 🖉 🖕						
Apply & display filter .						Expression.
3797 33.393304	Source	Destination	* Protocol	Length info		
3797 33.393364	192.168.15.138	62.210.217.267	TOP	B2 41846 - 9881	[ACM] Seq=256148 Ack=28:	18271 M1#=65535 Len=8
3800 33.397917	192.168.15.138	62.210.217.267	TOP		[ACM] 5eq=256148 Ack=283	
3803 33.481268	192.168.15.138	82.210.217.287	TOP		[ACK] 5eq=256148 Ack=283	
3804 33,481993	192.168.15.138	62.210.217.267	Tor			ck=2823951 Win=65535 Len
3896 33,482454	192.168.15.138	62.219.217.287	Tor	1139 41640 - 8881	[PSH, ACK] Seq=250683 A	ck=2823951 Win=65535 Len
3608 33,41268 3898 33,41268 3894 33,401993 3696 33,462454 3613 33,411946 3615 33,427725	192.108.15.130	62,218,217,267	TCP	07 41040 - 1001	[ACK] Seg=257748 Ack+28	20031 Min-65030 Lenv6
3815 33,427725	102.168.15.130	62.310.217.207	Tor			ck=2830032 Min=65535 Len
3819 33,438277	102.168.15.130	62.210.217.207	TOP		[ACK] 54g=258283 Ack=283	
3822 33,458998	192.168.15.130	62.210.217.207	TOP		[ACK] Seg=258283 Ack=283	
3824 33,487454	192.168.15.139	62.210.217.207	Tor			ck=2637132 Win=65535 Len
3828 33,491379	192,168,15,138	67.210.217.287	TOP		[ACK] 5eg=258826 Ack=28	
Arrival Time: 1 [Time shift for Epoch Time: 15 [Time delta fro	Mar 26, 2018 11:45:1: r this packet: 8.888 22989912 283375688 s on previous captured	(abnocea 900900 econds	seconds]			
Time shift for Epoch Time: 15: Time delta fr Time delta fr Time delta fr Time since re Frame Number: Frame Length Gapture Length (Frame 1s igno Protocols in Coloring Rule [Coloring Rule	r this packet: 0.000 22000012.283375000 so mo previous captured ference or first fra 301 02 bytes (656 bits) 02 bytes (656 bit	100000 seconds) frame: 0.000027000 i d frame: 0.000027000 mr; 33.407072000 seco) :Lp:top] :sc0c:29103:49110), Do	seconds] onds]		11d;5a)	

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]



ADP1 Protocol Bre	ala diresan				
Tor		5.83 MB	[99.0 %]		
Unknown		1.24 KB	[< 1 ft]		
DHCIVE MDNS		1.21 KB 738 Bytes	[< 1 %]		
NTP		354 Bytes	[< 1 %]		
Top nDPI Flows					
Vmware_c0:00:08 / 192.168.15.130 / 192.168.15.130 /	52.210.217.207 [Tor] 16c:db6b / ff62:11:2 Broadcast [Unknow 224.0.0.251 [MDN5]		KB [5.2 %] 1.21 KB [< 1 %] 500 Bytes 460 Bytes 85 [< 1 %]	$\begin{bmatrix} < 1 & 5 \\ [< 1 & 3 \end{bmatrix}$	
91,189,04,4 / 192	168.15.138 [NTP]	Z/e Byt	236 Bytes 118 Sytes	[< 1 %] [< 1 %]	
62.210.217.207 /	192.188.15.138 [Unknow	n] 68 Byte	118 Sytes s [< 1 %]	Te 1 m1	
2					
4					
2					
righlight.					
					Clear
-		E. 10. E	OPI Protocol s		

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

nterfac	STATE OF STREET	0 5 8 2		à 📕	G 2 B
I Ap	ply a display filter	<cri>/></cri>			Expression
NO.	Time	Source	Destination	Protocol	Length Info
100	1 8.888868	192.168.15.138	62.219.217.287	TCP	102 41846 - 9001 [SYN] Seq=8 Win=29200 Len=0 MSS=1468 SACK_PERM
	2 0.251801	62.218.217.207	192.168.15.130	TCP	88 9991 - 41846 [SYN, ACK] Sep=8 Ack=1 Win=64248 Len=8 MSS=146
	3 0.251852	192.168.15.130	62.218.217.297	TCP	82 41046 - 9001 [ACK] Seq=1 Ack=1 Win=29200 Len=0
	4 0.252419	192.168.15.130	62.218.217.297	Tor	289 41846 - 9001 [PSH, ACK] Seq=1 Ack=1 Min=29200 Len=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

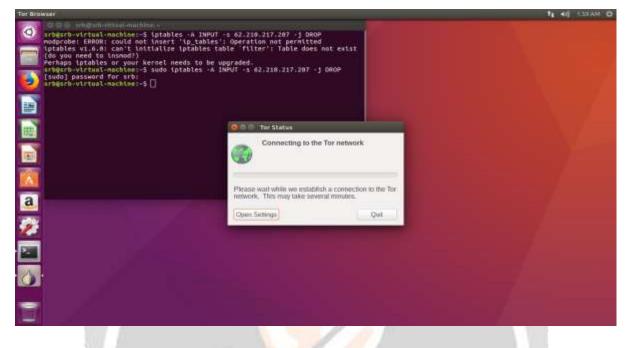


Fig -21: Blocking TOR IP using iptables

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

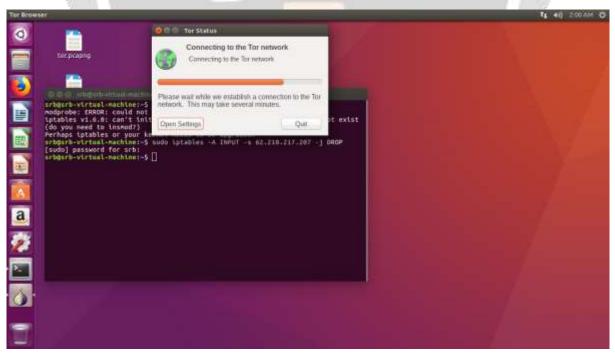


Fig -22: TOR trying to establish connection

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

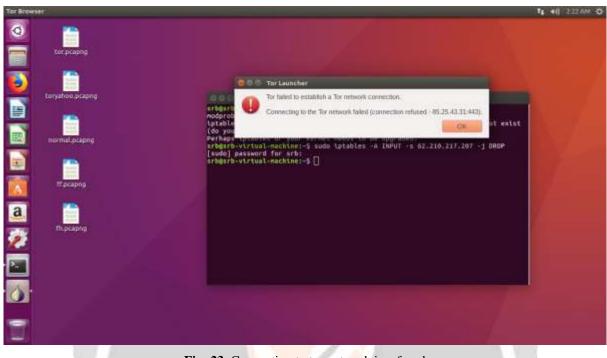


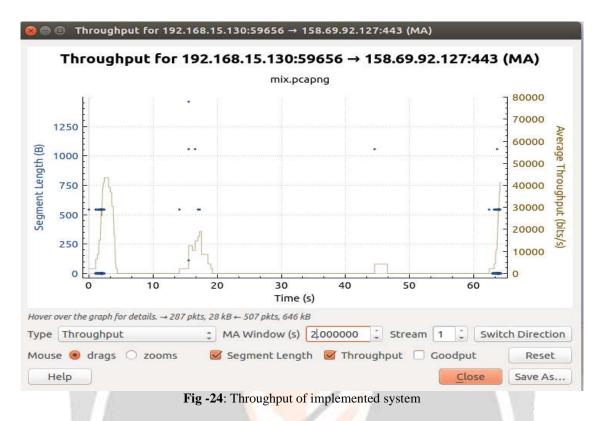
Fig -23: Connection to tor network is refused

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.



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.

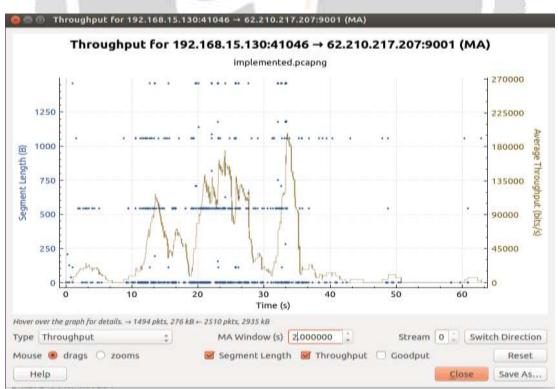


Fig -25: Throughput of implemented system

4399

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 <<u>https://www.geeksforgeeks.org/basics-computer-</u>networking/>
- [2] Networking Equipment. Accessed by 12 January 2018 at <<u>http://www.networking-basics.net/</u>>
- [3] Define Deep Packet Inspection. Accessed by 27 January 2017 at <<u>https://en.wikipedia.org/wiki/Deep_packet_inspection</u>>
- [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.