

ISSN: 2454-132X Impact factor: 4.295 (Volume 4, Issue 3) Available online at: www.ijariit.com

Network monitoring with open source packet sniffer

Rakhi Shrawat

<u>rakhi.shrawat786@gmail.com</u> Hindu College of Engineering, Sonepat, Haryana

ABSTRACT

Computer Network is a growing field every day. Networking has made life easy. Computer networks always have a big risk of security problems. However, to better understand real problems in a network and to solve them, it's important to go to the packet level. It is believed that all network problems arise from the packet level. This is where packet analysis plays a big role in computer networks. Network analysis, protocol analysis or simply sniffing are the other names of packet analysis. The purpose of this research paper is to monitor and analyze the network traffic packets of various protocols like TCP/IP, HTTP, ARP, ICMP etc. using a tool called Wireshark. Wireshark is a free and open - source packet analyzer. To analyze the packets of different protocols we are using different parameters are frame no. frame length, IP source, IP destination, header length of the packets and also window size value etc.

Keywords: Protocols, Wireshark, Packet Flow, Packet Capture, Network Monitoring, Network Analysis, Packet Sniffing.

1. INTRODUCTION

All network problems start at the core within packets. This is why packet analysis, also referred to as packet sniffing or protocol analysis is used to understand the basics of information traveling across a network. Packet sniffing is used to help maintain a network, comprehend network characteristics, discover who is using a specific network and their peak usage times, and most importantly pinpoint potential malicious attacks and activity. Whenever you connect to the Internet, you are dialing into a network hosted by an Internet Service Provider (ISP) which communicates with other networks. Packet sniffing allows all data within those communications between different ISPs and networks to be viewed, copied, and analyzed. Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues. [1]

2. HISTORY

In the late 1990s, Gerald Combs, a computer science graduate of the University of Missouri–Kansas City, was working for a small Internet service provider.[2] The commercial protocol analysis products at that time were priced around \$1500 and did not run on the company's primary platforms (Solaris and Linux), so Combs began writing Ethereal and released the first version around 1998.[3] However, he did not own the Ethereal trademark, so he changed the name to Wireshark.

3. EXPERIMENTAL SETUP

Analysis of the network performance of a given set of websites is done, using Wireshark software as a tool, I have captured packets of websites of the news channel. The set of websites include a website of a news channel and a website for live streaming. I have captured packets of images and audio from the news channel website and I've also captured packets from the live stream website while streaming for 10 minutes on my home network.

4.VARIOUS PROTOCOLS DETECTED IN WIRESHARK FROM A LIVE NETWORK AND WORKING OF THESE PROTOCOLS

While capturing packets from a network interface, Wireshark captures all of the packets coming and going over the network. Wireshark provides capture and display. Filters allow you to specify exactly which packets you have available for analysis. Simply stated, a filter is an expression that defines criteria for the inclusion or exclusion of packets. If there are packets you don't want to see, you can write a filter that gets rid of them. If there are packets you want to see exclusively, you can write a filter that shows only those packets.

Shrawat Rakhi; International Journal of Advance Research, Ideas and Innovations in Technology Protocols during capturing of the live network:

- TCP/IP,
- HTTP,
- ARP,
- ICMP Protocol.

	001000222		20 (LOCAL) ()		_	-
For- Dati Itian. Itia Cepture Unit	de . Joseffen .: Telepte	w 00.0	her hain they			
##1# 0088 9+	* 17122	= 19 I	5. 45 世			
Charles many the school of				E1 -) B	-	
1 THE SALE	The balance	-	Lange with			
3w1 45 (14)415 101-148 #-10	174-CER. DW-204	5011	AN ANTING A BE CADED SHART ADDRESSED Loads Plantamentations	(Tecretti)	DUNIT!	
3968 45. 342735 181. 188. 8. 8. 21.	174,129,289,288	WITH.	201 001 villests/setflin/fisiorapelliation.ed/fiack.version-fi	tesh tile 1.	pland).	-
348 45 234555 134 225 244 228	100,188,8.21	1908	do be + werse (word) heavy aptrology standalds (anot Thoul-Binder)	NR Taker-46	etter04	1
100 01.00010 174.005.000.000	107.040.0.31	wilt.	\$10-STRILL BD Parent Tenanterialy			
1947 85-34C512 041.008.0.02	274-128-288-2281	10.0	BLANDS BR (ACA) DARAGER AND ADDARD SERVICES SERVER TELEPORTE	DHE TROTA	118.811	251
- 188 85.252012 DRI 188.8.12	101101-0.1	10.0	IT Massians many listing a solution within an			
THE BLUTSPIE CALLAR X.C	CINEERS INCOME.	100111	THE PARTY AND ANT TRANSPORTED AND A TRANSPORT OF THE PARTY OF	GALLE CONTELL	211041	land of
108 08.377942 1411248.8.30	ALMAN MULT	308	ALLINES + 80 (SWI) Servel Adoresian prevent Patrianal-Sack_Photoa.	Classical144	ALL T	lan-
382 (05.207037 40.00.342,48	181:189.9.31	108	14 88 - 37883 [254], A24] 340-8 ALA-1 805-9782 184-8 785-1868	DACK_PERF-E	Trials	440
382 45.208385.182.088.8.20.	10.346.346.00	214	in pipels - W [ACC] dampi means simulated transf "Businessitions	2 Tao-iller	(141)	
101 05.210007 101.101.0.11	49.202.202.00		in an owned the solution of a second second second			
784-25-710209-03-88-242-48	10.4-941,192	10.0	BARA (1980) [MIC] Seard actual specific parent Paralitatificati	195 Parente	1253.0101	ь.
HE REALING & ALCOLUM	100.08.0.00	(B)	TINE TTP segment of a instantion this			
	-					
Moneys, 2n. 2002 These is advectived second (These is advectived second (These is advective) and (These is a second (These is second (These is a second (These is a second (These is a	, regarda, 36 deria					
		a a a a	and a second			
	网络建建物	8 X	attack etc.			

Fig. 1: Wireshark main window showing captured packets

i. TCP/IP

TCP/IP is not a single networking protocol – it is a suite of protocols named after the two most important protocols or layers within it – TCP and IP.TCP/IP is responsible for complete data connectivity and transmitting the data from end to end by providing other functions such as addressing, mapping and acknowledgment. The TCP layer handles the message part. The message is broken down into smaller units, called packets, which are then transmitted over the network. The packets are received by the corresponding TCP layer in the receiver and reassembled into the original message.

The IP layer is primarily concerned with the transmission portion. This is done by means of a unique IP address assigned to each and every active recipient on the network.

To establish a connection, TCP uses a three-way handshake. In the TCP connection establishment sequence, the opening TCP session sends a TCP datagram with the SYN bit set and the receiver sends a related TCP datagram with the SYN ACK bits set. A final ACK bit is sent from a sender to finish the TCP handshake.[4] It is shown in Figure 2. Frame 107 is the start of the three-way handshake whose sequence no. is 0 and after that in packet 111 when it gets acknowledgment from destination its sequence no. gets changed from 0 to 1.

	and the second se		
140	mand -	indictor from t	1947 25 ·
011 1.000011	THE REPORT OF THE PARTY OF	and states and states	HE REEL & MEDICIPAL CONC. INVESTIGATION CARRY INVESTIGATION AND PROVIDENCE
AND IN MORE	over productions	CARGE IN COMPLETE	and the product of a state of the state of t
111 1.8010	states (the first states, ittlessed),	and group in the Table	in all - and and all the many store of the store
122 1.001000	SHE'S DESCRIPTION OF A	we greger to when a	THE CONTRACTOR AND A DESCRIPTION OF A DE
THE R. LODGER	and Bully to a	page case (tag. 10	the association of and the first and a support of the same
111 P. Downey	and the first of the second se	passion. Co. 1	the same with the same state of the same state o
THE PLANE AND A	THE PARTY OF THE P	and the second second	the second second second second second little second secon
CAS P. DEBREN	the programmer and	see and the later	the construction of the standard states and the
LU P. LITTER	The second second second second second	and the second s	LA SET & REPORT OF LAND STATUS STATUS TO A STATUS
Contraction of the local division of the loc	test in the state of the state	and the second s	and they we have been able that have been approximately and the second stands
TT- Classes	ANT OF THE OWNER.	the deside of the other	the spectrum of the second second second second second second second
The property of	The firster in	and a second sec	is submitted a state total sub-total supervise strength these
and b. Contract.	term and that they want the	and the second second	the second second stand stand second second second second stands
and a constant	- and the radio of the second second	and property of the local sectors of the local sect	in and a sublicity that when a natural relation rate
and all presents	The second secon	page (per) the . The state	PARTICIPATION OF THE CONTROL OF THE CONT
one h install	And only they a built had a lot	and the second second	the start - when when it is an end of a start of a star
and h courses	- and the second second second second	and an other states of the second sec	and a second sec
and buildings	the part of the second second second	Links and the second	The second second second second second second second second
THE D. LOUGHT	and project the second s		
	and the second se	and the second second	
and he had been	AND AND INCOME.	The second second	To All a second second second and second and second second
NO OCTOBERT	The loss of the	in the lot has work in	The second s
and out wanted	the state and state	been week of page 76 and 10	and design of the large
· JOI 1 III STATE	IN ACCOUNTS OF A DAMAGE AND	sares yes him, on proofs	No. 2010 Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contraction Contra
网络拉斯拉马	Disconstantia di 18 della d	THE HET REPAREMENTS OF A	1 181 HE (HE 191 HE HEF)
HART PRODUCES IN	rates by from half-perchast shite	OUTLASS ATTA PART (1981)	INC Variation and and a series of the news , for a set graph and the series will a series
Addapted States	Press and a loss Party Intel 1995	CODE CONTRACTOR CONTRACTOR IN	

Fig. 2: TCP/IP Protocol connection establishment

1	Prese 2071 BB hyles on wire (NBB hilts), BB hyles captured (NBB hilts) on Interface #
h	etherset 13, who differently departed etherseful, but (bighted three to depart the lands the lands the lands)
i	Internet Without Works 5, 500 DBS (00. Data the state and parts and parts and the state with stare with stare and a reaction on these state and the state and
	Preventiation Control Pretaral, Ser Party MELLS for Party return 1440, San B. Lant #
	Same Fort Ball (Ball)
	Earthatter Series Street (AAV)
	Division function at the
	The second last of
	Too address your wi
	permit menter a (relative server)
	Actional Actions of Academy (B
	3888
	> Flags: work (EVS)
	sindre size velue: 6192
	[falcalated sideou shu: 3002]
	Checksami ductini (anverified)
	[Decktas Salary Berny Henry
	Read model 8

) Options: (13 bytel), fundame segment size, No-Operation (NOP), shoke scale, No-Operation (NOP), No-Operation (NOP), SACH presitted

	Frank that 54 monte on also (100 monte), 78 monte names of 500 kDec) on interface #
r	Proved 11, No. (Disarts Monorf (Origina, Monorf), No. Statutes 11, No. 4, Society (Disart)
	interest frances average a see and and that the shift also average and that the the shift also all and and the shift also all and and the shift also all and and and and all also all also all and and all also
	Constitutes Carbon Statistic Statistics and April 1997 1997 1998 1997 1998 1997 1998 1997 1998 1997
	denormality services of the service
	Sector rent and Sector
	Section with state (set)
	Drose spices d
	T27 Segnart Latu 4
	Infarten nation: 1. (relation importer matter)
	actionalization restart 1 (value) as moders.
	1940
	(Tart then (an))
	Charles the charles like
	Thrankful slother Hall broke
	[minute the shifts Party [26]
	Enclant BillPT [invertPiel]
	[Desidual (Malata Error 4/24)]
	transf adjuster) a
	1 Marriella and all all
	- Teatherst Westback

Fig. 4: Details of frame 111

ii. HTTP

HTTP functions as a request-response protocol in the client-server computing model. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content, or performs other functions on behalf of the client, returns a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body. [5]

As shown in Figure 4, packet 205 source sends a request to destination for HTTP and in response, it receives GET message in packet 214 after receiving acknowledgment. And at packet 215, the conversation is completed by the HTTP/1.1 message. The Web server responds in HTTP/1.1 with status code -302 found, which indicates to the browser that the target resource resides temporarily under a different URI.

Sec. 1	Tana .		
	and an investment of	and their load date in latter	in factor (fraction) into (FRE
100.01.0000	white the set of the set	and other land along a light	the balance characteristic year office
10.11.20.00	ALC: NO. 10 - 10 - 10 - 10 - 10 - 10 - 10 - 10	100 100 Last \$614 L \$100 -	- Del Martenez Lifer Calenda, Phys. State 1
PG.14.80.00	1981 APR DESCRIPTION	NUMBER OF STREET	and by loss the party, but it's the supervised and and
	-100.00 A.200	the second statistics of the	The basic of the participation of the participation of the same state of the same
0.0.000	100.000	NUMBER OF THE OWNER OF T	- 10 Max - management town where we wanted and the last we
	Contraction of the local data	the set of the set of the set	the start is not a set of the second second of the second se
	CONTRACTOR DATE:	the second s	THE PERSON OF THE OWNER WAS ADDRESSED AND ADDRESSED.
and the second	the second second second second second	and the second se	The second of the second
- DO CHER	10.001.00	and the second second second	and the second second second second second second second
122 111	the set of the	the star has said the start of	
	the second second second	and the second second	The second se
10001000	the local line	the second se	the set of
the base	10, 00, 1, 000	the set the off one that it	and the second sec
the in house	10,001,000	and the second second	and the second se
1.0.10.00000	Freedor Land & State on Lands.	141 Del 1 - 180 1 - 1 - 80°0	the stretch of the large base based
COLUMN ADDRESS	CONTRACTOR OF A	And the low on the London of	THE REAL PROPERTY AND ADDRESS OF ADDRES
	101 001 1 00	an last the last the second	and part of the pa
	B SIE		

Fig. 5: HTTP Protocol

As shown in Figure 6, at packet 10551 client receives a response in getting the message. At packet 10562 the Web server responds in HTTP/1.1 with status code -200 OK, which indicates to the browser that the object was successfully fetched

				I C C Spread
Tor Tor 104 204	Provide an analysis of the second sec	41844 4175 4175 4175 4170 4170 4170 4170 4170 4170 4170 4170	đ.	(a) Sector () (b) (b) (b) (b) (b) (b) (b) (b) (b) (b)

Fig. 6: HTTP Protocol

iii. ARP

The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given network layer address, typically an IPv4 address.[6] This mapping is a critical function in the suite. On seeing the capture file seen below in Figure 7, packets collected by it shows in packet no. 518 source computer is sending a packet to IP address 192.168.1.100 asking who has 192.168.1.1 address?

BUC DE ALLERS	And a send of the board of the	Matchinester	4004100	of magner located as the ball of the contract of the location
108.14/940315	Littlering parently	Wrettoalt.	40	100 pero Rea 200 100.1 (0 foto 100.300 1000
100.14.000.001	Angle Contents	a depart for the second of	111	- No. 2011 (2011) (2) (2) (2) (2) (2) (2011) (2) (2) (2) (2) (2)
THE DOMESTIC	261,000,0.196	Apple new matrix information and apples are	7094.4	the application loss
EX. 74.088838	-343,3880,3,389	341,448,318,209	1999	12 Name gamp 48 1341401980
525 76/404842	"Rome - binds: \$2291-back\$179.00	CHARGE REPORT	-1094	de trante é auto terto x bidde.
Sel skyletette	material 4, 4 mil	1014 (W. W. 1911		di manishi quela sirtuk 4 custari
100.16,681786	****	344.200.200.200	deal .	HERE BRANK COMMINST A BUILDING
LUI 76, 197111.	Testin - brief, 1200; weathy them	14621128	309HL	40 fulliment ultrianen feanry /ierzage sit
EE 74 (198448 -	100 100 1 100 V	Lang-recent set	100114	of materiality report 1 same given AM A.A. (20)
NOT 24 (1993)	Cognete, Lot Month	manual contraction of the second seco	140	-00 after haar 1001-1001-1-3007 1433- 833-448-1-0
Kall 74,76088	Advention of the second	Gingham in the st	.AMP	the self-time in the terms are served in the product of the
THE PROPERTY.	Name - Adapt, 12251 + 44251 - 18455	44821100	TIP-1	of the bound of the second process of

Fig. 7: ARP Protocol asking who has 192.168.1.1 address

In figure 7, ARP Protocol asking who has 192.168.1.1 address it also provides functionality to find client's layer 3 address by allowing transmitting computer to send ARP broadcast. A computer that has IP address will identify itself by sending a response containing its layer 2 address back to transmitting computer. The second packet in Figure 7, Packet 519 shows destination computer's ARP response to the first packet. In response packet no. 519 shows that the above address 192.168.1.1 is at bc:8a:e8:12:3b:a3 machine(MAC address)..If there is no response from the host, it may not be present on the network.

iv. ICMP

The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating [7], as shown in Figure 8, a requested service is not available or that a host or router could not be reached. Computer send echo request, it should receive echo reply in response but in some cases, TTL time exceeded ICMP message is sent when the TTL value of an IP packet reaches zero. In normal operation, a network should not have a diameter so great that the TTL gets reduced to zero. The most common occurrence of this is when there is a routing loop. In this case, as the packet is sent back and forth between the looping points, the TTL keeps getting decremented until it reaches zero. That's when this message is sent.



Fig. 8: ICMP Protocol

5. GRAPHS AND OTHER PROPERTIES RELATED TO THE CAPTURED PACKETS



Fig. 9: Time Sequence Graph of the captured packets



Fig. 11: Throughput Graph of the captured packets



Fig. 10: Time Sequence Graph of the captured packets



Fig. 12: Throughput Graph of the captured packets

Neic / Itee	Cauet.	Average	No. val	No.val.	Arté (wi)	Fercent	lucat rate.	Bent star
ITTP Requests by Server	-08				0.0001	30es	8.8506	04.000
1077 Requests by Server Millions	48				0.0001	108.805	6.0509	66,608
172.16.32.198	24				0.0000	88.885	8,8038	2.587
MELBACAG-ProvE1: NERS	24				0.0000	108.815	0.0100	2.387
580.343.328.335	£				0.0000	12.588	0.0108	64,708
5840-80-48445-cow	3				0.0000	208.805	8.8356	64.793
25.23.258.85	4				0.0000	10.085	8.0109	5.618
pling.thartbest.net	4				10.0000	109. MIS	0.0100	5.618
111.212.25.15	3				0.0008	7.565	0.0500	44,600
101.001.000	1				0.0000	100.005	8.0008	14,638
21.241-128.08	4				0.0000	2,505	0.0104	63.4M
same minted, now, and	1				0.0000	104,805	8.2198	65.014
218, 104, 218, 151	T.				9.0000	2,509	0.0500	68,883
COPULATION CONTACT					9.0000	104,605	0.0109	56,687
283.11.171.189	T				8.000	2,985	6.0226	04.718
repairs dor. Service Ideality, non-	1				0.0000	100.005	0.0100	54,710
511, 221, 29, 13	1				9.0000	2.595	0.0109	75,306
8.800 cm	1				15.0000	104,915	10.07298	78.209
TTP Bemarks by WTP must	40				0.0081	108.805	0.25288	14,108
RELEACES-Rough (1994)	14				0.0000	phy control	6.0006	2 187
122.06-02.136	24				10.00000	trial aire	4.0104	2.102
alsolath, adventions					10.00000	12.586	8.0708	AL 1978
183, 263, 230, 231	1.0				10.0000	104 205	6, 6008	54.755
also charthat out					10.0000	104.4085	8.6104	5.498
11, 21, 130, W					0.0000	101.005	6.0100	5.038
077 BEL 208	1				0.0000	1.506	0.0100	12.008
111 221 29.36	8				II. Only and	104.005	0.0100	14,610
one often real and	1				0.000	3 505	1. 10.00	15 414
23, 300, 274, 99	1				0.0000	108.805	6.0108	10.404
income the Importantia can	1				a	3 108	0.0100	14.718
285.12.271.204	1				0.0000	108.000	0.0100	18.718

Fig. 13: Load Distribution of the captured packets

C Theat disk - conc - Tempert								
File Dati Formul time. Help								
WWW.cont Historication			1000					
Tando / Itua	Team .	BARTAGE.	Also well	Res and	Rate Incl	Foregate	Barat rates	Berry start
and the second								
HTP Reports by Reven	-2014				6.000.7	31475	#.30en	318.818
#170 Reports by Serier Athens	259				8,8085	308,905	8,2080	318,818
13.107.4.10	1214				8.0082	10.075	0.2000	318,818
2. Kis. dl. oklivery. an microsoft.com	85				8.8091	45,188	4,5460	218-010
7. #1. dellovery .mp. microsofttam	15				8,8080	23.108	8,8580	326:453
dl. siellowry.ms.misrowstit.com					6.0000	1.111	0.0100	346.759
188-142-171-14	40				#.80HT	20.025	8,2680	323,894
J.T.L. R. mellivery an and rocovt.cam					8.0001	1008.0075	8,8480	121.998
184.14.244.75	35				F. BUNKS	1.175	9.0000	300.509
store constant a station of the	10.				8.8000	104.000	8,8280	206,898
127, 18, 18, 180					B. B1997	1.043	8.0100	82.789
#1174CH1-Tro.#1-9090					#.809b	100 200	8.0100	82.786
18.8.21.18					R. manual	1.805	0.0200	215.076
contracted at att, however, 1,0014					8.0000	tone, Ann.	0.0000	265.879
115.19.47.238	1.0				6.0000	1.605	0.0400	214 344
1. Mar. 41. delivery an alternative can					E. BURD	200.000	0.0000	218,218
A 355 URL 200					# . WORKS	1.725	8.8280	118, 111
7. 41 children and advectment time.	- C				a shorter	1000 0000	8 8180	214, 273
133.09.07.127					6.0000	TO THE	10.01.00	113.003
3. 43. doi:10.000 and anti-proposition from					a analy	100.000	8.0100	319,823
11. 6. 41.27	- T				8,8080	1,345	8.4189	127.654
h month and	180 - E				#	10.700	10.000	120. 202
and the second state when	- C				A	NO. UTD.	A. 101 Mar.	101.00
states, or in the superior of the	4				R. WORK	TT. STE	a. 0100	123.353
10 Mill and and	-t-				a. 201000	31,000	4. 81.00	448.000
and an and a set of the set of th					A 10000	THE APPLY	A 0.5 MAY	where where
107 18 217 20					P. (0)(0)	1,200	8.0000	100 100
the first offerthe sold strength	1.5				2. August	ALC: NOTE: N	A. 41444	1014 0018
a 101 101 140	- C				N. 10000		10.000 M	220.274
Contraction of the second second	1					8 1 80/08		110, 104
A BY ONLY WY AND ANY YOUNT, I'M	10 C					1000.000		114.314

Fig. 14: Load Distribution of the captured packets

enty.	Turmeny	Owner .	Frederad.	Ceurit			115.75.115.55.7					-
Date	They forget an ever spectral safe transmission To	Lighterman	TCF	The second second	1 C	Packat Hestname	Content Type	Size	Filenary			
bonge .	Haltonned Becker (Dicastion erstand)	Matumat	HTH	8.		1662981 man is only come	and enters is soon from other ended	1797 Judei	marilate	inine relation	Sec.	
b Million	Connection and (MIT)	Sequence	TCP -	59		Second percentions	Manufacture a contraction of the second	the second	Parices.	and the first	10.14 miles	
a ning	NOF Zero Webbo (wpriere)	Seguence	100			166339 perch-conv.com	epplication (san	10 Eyres	pentati	HMML_CDR.	(現,祥明)	10112
aning.	Review segmential not captured common at capture the	Sequence	104	8		168364 Ibuildgyte.com	application/octet-cheam	6 bytes	134 mm	a to Schull?	42281	
2010	This fitame is a jourgested; out-at-order organist	Sequence	309	38		166375 th address rates	anolication/ortat.stagen	6 budget	122.00	and detailed	81129	
and and	Maked ApppE segment wells "ITB" Identifies and Taxatel	Mathematics.	Bill (#15) mage	W).		second strangerster	abburner to construct the second	2534.5				11
-	Ignored Delivered Percent	Patient	- 14 -	•		REAL PERSON PLANNING OF	application/red apple impegial	TTG1 EAder	14540,70	u'w-burg	00146-10	(HED)
-	. TCP senders specified by the sense is new completely full	Sequence .	108	0		169711 hiedubp-lhakamahd.net	video/mp/t	544 hB	segret	(152854019	100,00-0	to Test
64	Duplicate ACK (#1)	Sequence	108	161		166016 th address cores	application/octet-theam	5 better.	This rest.	abotal?	17694	
H.	Burnated Tag Langth	Material	OUC	1		140010	in third	THE MOON			1000	
E .	This hartwise a like pochsic ten anamasian	Sequence	10	100		100710	100/10/00	are bitter	1.1.	1	10.00 m	
N	This Peake is a bruggerbuilt sporteur refresombation	September	TOP	81		168923 TB-M#[[p07.0041	application/octet-stream	> D bytes	132,000	#10Xb=93	2000	
66 - C	Duglicani ASK (#2)	Sequence	102			168928 Ib widework pers	application/octet-statemy.	. 6 bates	134 (184)	a tolchod?	40670	
N	This section means premisely regarized keys Cleaner me	Sequence	19.	1		WERE his fide, it shows that and	hopficiation/and angle more and	TREE budges	Lordan 20	Concernition (1)	10.00.00	
Ni	TCP beep with a sugment	Sequence .	10			100104 revenuer matematicate	Where we we we will be a feature	and the second	140,3	o be breeze	Norsele in	UPED!
N0	(Deplines ACK (93)	Sequence	TCR	0		163422 Hendladsp-th-akternethil.net	wdeo/wp25	47018	ingrier	(15)2814830	340,004	11714
hé .	Digitizate ACK (#4)	Sequence	109	×		167425 Illi vidigyor.com	application/octet itream	5 bytes	134,000	and the St	12201	
	Depircule ACK (#0)	Lequence	TCP	1.		167345 man bucks com	interference in the second sec	1801 butter	- Aller	and a state	Sec. 2	أرجعه
÷	Displicate GCK (PR)	Seigence .	10.0			in the part is the control of	Shorter to a second		124	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	and special	100.00
in the second	Displicate ACE (PT)	Septemb	119	孝.		10/441 IB MERVICENT	application/ octor strains	to tryines	124,000	ALTHICKNESS	110he	
*	Duplicate ACK (HIL)	Segurate	109	8		167443 penth concorn	application/post	18 bytes:	perfitt	serve table	di spek;	tata)
46	ACK to a TCP logs all a segment	Segrence	TCF	R.		167,852 He understory open	anterior adversed by that a strengthen	6 butter	12 met	a tobe book	15296	
100	Deplicate ACK (#8)	Separat	11.8	10 C		artada in ca	the second second second	d home	120.011	10.24.05	11.172	
100	HTTP body rebitionatur televit meng teersitic subdicactor	Married.	- Pettine	<u>.</u>		10.400 is sugger.com	abboration/ possi-tearan	a show	124000	With Chicks	0114	
266	The admonifestgment mariter field to ministero while the Au-	Protectol	10	<i>R</i> .		16/473. hindidbp-Ihuskamahd.net	application/vitd.apple.mpage#	3381 bytes	index_33	0,00-2.003	a@hdc30	inbi
ы	This have is a burpaction failt at an annumenco.	Sequence	TOP	<u>n</u>		167922 hindigbo-hukamahdinat	wdeo/wa0t	53248	caornant	153854821	300 40-5	ichid.
100	Digitization (ACR) (#103	Dequerra	10	<u>#</u>		-school is under some	and the second states	C. burbart	100.000	1.1.1.1.1	and the second	
040	Displicate WCR (#11)	bequence .	11.0	<u>.</u>		inves managerent	approximation contacts	o spice	Country.	With Other	19114	
104	Depticula ACK (#12)	SAQUENCE	10.0	÷.		168041 Ib solgyor.com	application/jocitet-chinarty	6 bytes	134-ptp	a telsta lä	11280	
	Dupticate DCE (#12)	Dequence.	11.0			168088 Ib edgeor.com	equilantics/octet-cheam.	fi bytes	134 state	a to be to all	4234	
	Explorate AUX (F14)	Supreme .	10.	2 -		1000771 bindiabe, it also and and	involution and another months of	2001 Puters	Index 10	for such	diant-17	
T	Defection of a liable	PER-	157	2		Contract of the second second second second	although the ship of the first sector	100.00				
	Deligional erce in Mi	Destruction of the	10	*	2.00	10057) handwop-husbarrahd.net	ingeo (altri)	362.88	segment	(ISCIDENCE)	,300,8e-b	Votes.
that an						(c))						1.00





dat 10.ac 83 dat 10.ac 83 dat 10.ac 84 dat 10.ac 85 dat 10.ac 85 dat 10.ac 85 dat 10.ac 85	25 106 H 4407 8 774 9 108 24 202 3 500	2 8 8 8 8 8 9		21 38 9	1100 82,917225 0012 80,11000 174 00,101902	71,3478 75,1867 85,4878		
dar Monchol dar Monchol dar Monchol dar Monchol dar Monchol dar Monchol	8 ALT2 8 TA 9 TB 34 3620 3 360	8 8 8 9	1	*	##12 \$1.11008 774 \$4.301502	75.1382	H.	
da Boudd da Nordd da Nordd da Mordd da Mordd	8 TM 9 188 34 3620 3 360	*		*	T74 84,809602	-09-18/M		
da: Muscht da: Muscht da: Muscht da: Muscht	9 188 24 2622 3 360			1.0				
de Marda de Marda de Marda	34 3422				188 FL304097	00.5017	ar .	
de Mor Mi de Nor Mi	3 . 30			34	2020 BLWEIMAN	T1.0481		
the block of		.0.		1.1	300 EL455064	007942	0.0	
	100 BA22	10			Mill BLADERT	75.1001	0	
dicition with	3 254			3	234 BE soderil?	102307	0.	
da Macile	8 485				408 83.302794	643036	(kr)	
de Manifel	4 588		B		000 ht.meet.et	31.0071		
dailhachd 19	4,2175 (1)(14)	122,588	142.94	46,000	7954 8400088	27112448	778.4	20
*****	4 302	-4	332		> NUMBER	STEMP.	(4)	
111111	38 9706	80.	1794	00	P KENDING	19884-0011	-47	
	da Mucist da Mucist da Mucist da Mucist da Mucist da Mucist da Mucist	de Maasto & Auto Adabaanta & Alde Aashaanta & Alde Aashaanta Hagama (Alama Marka & Alama Aashaanta & Alama Aashaa Aashaanta & Alama Aashaa	An Marceston B. 2020 O Ball Marcell B. B. 2010 Ball Marcell B. BETTS 199100 T22,584 Annest A. 2022 A Annest BB 8756 B0.	la Blacket θ alle 0 θ Ballacket θ 600 0 0 Ballacket H 107 (1989) 122,584 (16754 Heres 4 202 4 322 Anne 10 4200 00 7779 Heres 10 4200 00 7779	la Bhacada 8 ang Bahacada 8 ang Bah	la Musco 6 ant 0 6 6 ant 83.000 la Musco 6 60 0 5 5 000 Kaneter la Musco 7 1910 122,94 147 M 42.11 796-6.0000 new 4 202 4 202 6 8 82.5000 new 8 202 6 0 1779 0 0 82.5000 new 9 6 5756 60 1779 0 0 82.5000	at Hunces 6 and 0 6 6 4 446 ELLCOPE (05,505 ablanced 8 080 0. 0 6 500 ablanced 8 1020 ablance 1 1020 ablance 1 1020 10204 1020 1020 10204 1020 1020 10204 10204 1020 10204 10204	a H March 6 Ann 0 6 6 Ann 25 XC (20 05 XC 0) a H March 6 00 X 0 5 00 a H March 7 10 12 XM (10 ² M 10 XC 1) 755 - 1400000 (10712) MH Here 4 202 A 302 C 10 12 XM (10 ² M 10 XC 1) Here 6 A 302 A 302 C 10 12 XM (10 ² M 10 XC 1) Here 7 X 10 10 10 10 10 10 10 10 10 10 10 10 10

Fig. 17: Conversation Window





Fig. 18: I/O Graph of captured packets

Fig. 19: Capture File Properties Window

6. CONCLUSION

In this paper network traffic from a live network is shown by monitoring and analysis on that captured files and then statistics is built. Using Wireshark software was easy and convenient as it gave me a real understanding of network performance. Wireshark gives an option in which we get the object list of the packets we captured or say a user who is on the network using whatever sites they visit. Various graphs related to captured files are shown and other attractive features are shown which make Wireshark a great tool for network analysis. Among all the properties listed above, the most interesting one was Load Distribution. The output graphs generated through captured packets provides details of network performance. This paper helps in the practical understanding of network performance and applications.

7. REFERENCES

- [1] En.wikipedia.org. (2018). Wireshark. [online] Available at: https://en.wikipedia.org/wiki/Wireshark [Accessed 5 Apr. 2018].
- [2] Wireshark.org. (2018). 1.4. A brief history of Wireshark. [online] Available at: https://www.wireshark.org/docs/wsug_html_chunked/ChIntroHistory.html [Accessed 15 Apr. 2018].
- [3] Wireshark.org. (2018). 1.4. A brief history of Wireshark. [online] Available at: https://www.wireshark.org/docs/wsug_html_chunked/ChIntroHistory.html [Accessed 15 Apr. 2018].
- [4] Tcpipguide.com. (2018). The TCP/IP Guide TCP Connection Establishment Process: The "Three-Way Handshake". [online] Available at: http://www.tcpipguide.com/free/t_TCPConnectionEstablishmentProcessTheThreeWayHandsh-3.htm [Accessed 19 May. 2018].
- [5] En.wikipedia.org. (2018). Hypertext Transfer Protocol. [online] Available at: https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol [Accessed 21 May. 2018].
- [6] En.wikipedia.org. (2018). Address Resolution Protocol. [online] Available at: https://en.wikipedia.org/wiki/Address_Resolution_Protocol [Accessed 21 May. 2018].
- [7] En.wikipedia.org. (2018). Internet Control Message Protocol. [online] Available at: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol [Accessed 22 May. 2018].